EU FIUs` PLATFORM

MAPPING EXERCISE AND GAP ANALYSIS ON FIUs` POWERS AND OBSTACLES FOR OBTAINING AND EXCHANGING INFORMATION

Report

Project Team:

Traitement du Renseignement et Action Contre les Circuits Financiers Clandestins - TRACFIN, France

Unità di Informazione Finanziaria per l'Italia – UIF – Italy

Generalny Inspektor Informacji Finansowej – GIIF, Poland

Oficiul Nacional de Prevenire si Combatere a Spalarii Banilor – ONPCSB, Romania

Project Leader:

Unità di Informazione Finanziaria per l'Italia – UIF – Italy

Adopted by the EU FIUs' Platform on 15.12.2016

Disclaimer:
This report has been prepared by a project team in the context of the work of the EU FIU Platform for the sole purpose of providing to the European Commission a snap-shot of EU FIUs powers and obstacles for obtaining and exchanging information at a certain point in time.*
The report has been adopted at the EU FIU platform meeting on 15.12.2016. It is based on information collected in 2016 and it should be noted that there may have been regulatory developments in several Member States that are not reflected in the report.
The European Commission's support for the production of this report does not constitute endorsement of the contents. The report reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

*) An expert group that advises the Commission on Anti-Money Laundering and Terrorist Financing issues

SUMMARY

INTRODUCTION ..... **IV**

EXECUTIVE SUMMARY ..... **XIII**

CHAPTER 1. FIUs' domestic status and organisation **1**
1. Introduction 1
2. Institutional setting - Nature of the FIU and organisation where it is located 4
2.1 Administrative FIUs 5
2.2 Law enforcement and judicial FIUs 6
2.3 "Hybrid" FIUs 7
2.4 Conclusions 8
3. Additional functions carried out by FIUs 9
4. Resources 10
4.1 Human Resources 11
4.2 Financial Resources 12
4.2.1 Lack of autonomous budget 12
4.2.2 Autonomous budget 14
4.2.3 "Mixed" approaches 14
4.3 IT Resources 15
5. Governance 15
5.1 Internal organization – Organs and structure 15
5.2 Appointment and removal of the Head of the FIU 17
5.3 Decision making procedures 21
5.4 Accountability 22
6. Conclusions 24

CHAPTER 2. Operational autonomy and independence **27**
1. Introduction 27
2. Operational autonomy and independence in the exercise of FIUs' functions 28
2.1 Autonomy in the receipt of STRs/SARs 28
2.1.1 Interposition of other bodies 28
2.1.2 The FIU as the only recipient of STRs/SARs – Exclusive and multiple reporting 30
2.2 Autonomy in the analysis 32
2.2.1 Inception. Triggers and priorities 33
2.2.2 The analytical process 34
2.2.3 Conclusion of analysis 36
2.3 Autonomy in the dissemination 36
2.3.1 Independent decision to disseminate 38
2.3.2 Timing of dissemination 39
2.3.3 Recipient competent authorities 40
2.3.4 Disseminated information 41
2.3.5 Indications on priorities and possible follow-up 42
2.3.6 Procedure for dissemination 43
2.4 Autonomy in receiving or accessing threshold-based disclosures 43
2.5 Autonomy and operational independence in FIUs' powers 44
2.5.1 Autonomous access to external sources of information 44
2.5.2 Autonomous capacity to request and obtain information from obliged entities 45
2.6 Autonomy in cooperation with domestic authorities and other FIUs 48
2.6.1 Capacity to engage independently and exchange information with domestic authorities 48
2.6.2 Capacity to engage independently and exchange information with other FIUs 49
2.6.3 Autonomous capacity to suspend or withhold consent to suspicious transactions at the request of another EU FIU 50
2.7 Autonomy and independence in FIUs' organisation 51
3. Adequacy of resources 52
3.1 Conclusions on the adequacy of resources 55
4. Assignment and independent management of resources 55
4.1 Conclusions on assignment and management of resources 58
5. Links with external parties 59

5.1 Links with the host organization 59
5.2 Links with law enforcement agencies and prosecutors 60
5.3 Access to FIU's information by third parties 60
5.4 Conclusions on links with external parties and access to FIU's information 62

CHAPTER 3. Information received, available and accessible to FIUs 64
1. Introduction. Disclosures received on suspicious activities 64
1.1 Money laundering and "associated predicate offences" 66
2. Nature and use of disclosures on suspicions: STRs, SARs, UTRs 66
2.1 Structure and content of disclosures 69
2.2 Implications for the FIU's analysis (and international cooperation) 70
2.3 The reporting procedures: direct or through third parties 72
2.4 The reporting procedures: means and channels used 74
2.5 Timeframes for reporting suspicions 76
2.6 Conclusions on disclosures of suspicious activities 77
3. Other domestic disclosures received by FIUs: nature and content of threshold-based disclosures 78
3.1 Reporting procedures and timeframe for threshold-based disclosures 81
3.2 Conclusions on threshold-based disclosures 82
4. Access to "financial", "administrative" and "law enforcement" information. General aspects 84
4.1 General conclusions on FIUs access to "financial", "administrative" and "law enforcement" information 86
5. Financial and administrative information. Information on bank accounts through centralised databases or retrieval systems 87
5.1 Other means of accessing information on bank accounts 89
5.2 Conclusions on FIUs' capacity to determine the existence of bank accounts 90
6. Information on the identification of assets 91
6.1 Conclusions on access to information on the identification of assets 92
7. Information on legal and beneficial ownership. Central databases 93
7.1 Other information sources on legal and beneficial ownership 95
7.2 Conclusions on access to information on legal and beneficial ownership 95
8. Other financial and administrative information 96
8.1 Conclusions on access to other financial and administrative information 98
9. Law enforcement information 99
9.1 Types of law enforcement information 99
9.2 Access procedures 101
9.2.1 Direct access 101
9.2.2 Indirect access 102
9.2.3 Timeframe 102
9.3 Conclusions on the FIUs' access to law enforcement information 103

CHAPTER 4. FIUs' power to obtain information from obliged entities 104
1. Introduction. Scope and purpose 104
2. EU FIUs capacity to obtain information from obliged entities 106
3. Triggers and conditions 107
3.1 Broad capacity to obtain information from obliged entities 107
3.2 Existing conditionalities (existence of prior STRs/SARs; need for court orders) 108
4. Conclusions 110

CHAPTER 5. Domestic functions 112
1. Introduction. The analysis function of the FIU 112
2. Operational analysis 113
2.1 Capabilities regarding operational analysis 113
2.2 Separation between analysis and law enforcement activities 114
2.3 The scope of operational analysis 116
2.4 Operational analysis – tools and procedures 116
2.5 The capacity of FIUs to focus on relevant cases 117
2.6 Conclusions and challenges on the FIUs' capacity to focus on relevant cases 119
3. Results of operational analysis. Intelligence products suitable for use in investigations 120
4. Strategic analysis 121
4.1 Conclusions and challenges on strategic analysis 123
5. Dissemination to competent authorities (spontaneous) 124
5.1 Capacity to select the cases to disseminate 124

5.2 Capacity to select the information to disseminate; the recipient authorities 124
6. Capacity to provide information on request from competent authorities (dissemination on request) 129
7. Postponement of suspicious transactions 130
7.1 Capacity to postpone 130
7.2 Duration of postponement 131
7.3 Procedure 132
8. Conclusions 134

CHAPTER 6. Cooperation with other FIUs 137
1. General aspects 137
1.1 Capacity to exchange information 137
1.2 Purpose limitation: exchange for FIUs' analytical purposes 138
1.3 Purpose limitation: exchange on money laundering or terrorist financing cases 140
1.4 Police and judicial FIUs: separation between FIU's cooperation and law enforcement or judicial cooperation 141
1.5 Capacity to use domestic powers to obtain and provide information to foreign counterparts 143
1.6 Need for memoranda of understanding as a precondition to cooperate 144
1.7 Condition of reciprocity 145
1.8 Need for a clearance or authorization from a third party 150
1.9 Timeframe for responses. The issue of "timeliness" 152
1.9.1 Timeframe for responses. Factors that affect timeliness 153
2. Cases where the exchange of information can be refused 154
2.1 Cases for refusal to cooperate 156
2.2 Existence of investigations or legal proceedings 156
2.3 Identification and type of predicate offences 157
2.4 Motivated requests 159
2.5 Other factors 160
3. Completeness of the information shared 161
3.1 Sharing financial and administrative information 161
3.2 Sharing law enforcement information 163
4. Use of domestic powers to respond to requests from other EU FIUs 164
4.1 Legal basis (at national and EU level) to use domestic powers 165
4.2 Scope of available powers and existing limitations to their exercise on behalf of foreign FIUs 166
5. Cooperation in cross-border cases 169
5.1 Cross-border STRs/SARs 169
5.1.1 Legal basis for sharing cross-border STRs/SARs 170
5.1.2 Conditions and limitations to the sharing cross-border STRs/SARs 171
5.2 Obtaining and forwarding information from obliged entities established in the territory of the requested FIU and operating in another Member State 173
6. "Known/Unknown" exchanges 175
7. Matching of data sets 176
8. Joint analysis 177
8.1 Nature and purpose 177
8.2 Legal basis for joint analysis 178
8.3 Conditions and limitations to joint analysis 179
8.4 A supranational approach to FIU's cooperation – Towards a "Financial Intelligence Unit of the EU" 181
9. Obligations for requesting FIUs 184
9.1 Requirements for the requests 184
9.2 Use of the information exchanged 185
10. Consent for further use or dissemination of the information exchanged 187
10.1 Limits to the use and dissemination of the information exchanged. The prior consent 187
10.2 Capacity to provide the consent. General scope, limitations and conditions 189
10.3 The requested use or dissemination "falls beyond the scope of application of domestic AML/CFT provisions" 190
10.4 Existence of criminal investigations or legal proceedings in the country of the requested FIU 191
10.5 Impairment of a criminal investigation 192
10.6 Disproportion with legitimate interests and contrast with fundamental principles of national law 193
10.7 Tax-related cases or information 194
10.8 Other conditions 195
10.9 Conclusions and proposals 195
10.9.1 Re-casting cases of derogation to the consent 197

10.9.2 Consenting the dissemination to law enforcement agencies and prosecutors, not the use as evidence . 197
10.9.3 Use and dissemination for intelligence purposes 199

CHAPTER 7. Cooperation with non-FIU counterparts ("Diagonal Cooperation") 201
1. Introduction. "Diagonal" cooperation with foreign non-counterpart; features, modalities, difficulties 201
2. Capacity to exchange information with foreign counterparts that are not FIUs 204
3. Direct and indirect channels used for diagonal exchanges 205
3.1 Issues in the indirect "diagonal" cooperation for the exchange of police information 207
4. In case of direct exchanges, are the FIUs of the interested Member States informed? 208
5. Information that can be shared through diagonal cooperation 209
6. Possible use by foreign non-counterparts of the information shared 210
7. Lack of appropriate legal basis in support of diagonal cooperation 211
8. Conclusions and proposals 213

CHAPTER 8. Data protection, confidentiality, security 216
1. Introduction 216
2. Legal framework on confidentiality and security 217
3. Confidentiality and security requirements in the FIUs' functions 218
3.1 The receipt of data 218
3.2 The handling of data 219
3.3 Procedures for the access to external sources of information 219
3.4 Domestic dissemination of intelligence products 220
3.5 FIU-to-FIU exchanges 221
4. Confidentiality and security safeguards at the organisational level 221
4.1 Access to FIUs' facilities and protection of information security 221
4.2 Restricted access to IT systems managed by the FIU 222
5. Security clearance levels for staff and understanding of responsibilities in handling and disseminating the information 222
5.1 Security clearance for staff members 222
5.2 Screening of employees and recruits 223
5.3 The responsibility of FIU personnel to safeguard information 223
5.4 Training and awareness raising activities 224
6. Conclusions 224

CHAPTER 9. Most relevant problems or shortcomings encountered in FIU-to-FIU cooperation 226
1. Introduction 226
2. Difficulties deriving from differences in FIUs' status and powers 226
3. Need for a prior STR/SAR as a condition to provide cooperation 227
4. Refusal of cooperation due to the mere existence of investigations or legal proceedings 227
5. Refusal of cooperation due to the need to use law enforcement channels 227
6. Refusal of cooperation due the identification and type of predicate offences 228
7. Lack of capacity to obtain or share information 229
7.1 Lack of banking information 229
7.2 Insufficient capacity to obtain information and access databases 230
7.1 Insufficient capacity to obtain information from obliged entities 230
8. Insufficient capacity to provide the consent for further use or dissemination of the information exchanged 230
8.1 Limitations of the use to "intelligence purposes" only 232
9. Insufficiently motivated requests 232
10. Cooperation on terrorist financing 233
11. Cooperation on cross border cases 234
12. Innovative forms of cooperation 235
13. Lack of timely cooperation 235
14. Problems in cooperation in situations of postponement of transactions 236
15. Increase in FIUs' workload 237
16. Difficulties deriving from the absence of reciprocity 237
17. Use of FIU.NET 238

INTRODUCTION

1. Background and process

The "Platform of the Financial Intelligence Units of the European Union" (hereinafter referred to as "EU FIUs' Platform" or "Platform"), was set up in 2006 as a working group to discuss matters concerning the implementation of the provisions in Directive 2005/60/EC (Third AML/CFT Directive) of interest to FIUs and the improvement of cooperation among the FIUs of the EU. The Platform was subsequently formally recognised by the Directive (EU) 2015/849 (hereinafter referred to as the "Fourth Directive" or the "Directive"), whose article 51 sets out a detailed mandate including several objectives related to both "policy" areas (facilitate cooperation among FIUs, provide advice on implementation issues relevant for FIUs and reporting entities) and more practical or operational aspects (identification of suspicious transactions with a cross-border dimension, the standardisation of reporting formats, the joint analysis of cross-border cases, etc.).

Immediately after its inception, the Platform approved its initial Work Plan, outlining several work streams to pursue in a first round of activity. The Work Plan envisages a number of projects dedicated to the implementation of particular aspects of the EU framework related to FIUs' activities and cooperation. Work was initiated on, for example, a common understanding of the use of the information exchanged "for intelligence purposes", a shared definition of "cross-border" suspicious transaction reports, the conduction of joint analyses.

It was also immediately felt that the framework and practices of FIUs' cooperation in the EU is still affected by several shortcomings that impact on effective operations. Experience from the field (but also findings from evaluations conducted by the Financial Action Task Force – FATF and MONEYVAL) clearly demonstrate that despite the common framework based on international standards and EU provisions, FIUs continue to encounter significant difficulties in having access to information for their analysis, exchanging this information with foreign counterparts, develop effective action to prevent and deter money laundering and terrorist financing. In many cases, FIU-to-FIU cooperation is hindered by lack of information, absent capacity to exchange, constraints in consenting to its further use in investigations.

These concerns about the FIUs' capacity to prevent and disrupt money laundering and terrorist financing has become more acute following the terrorist attacks in 2015 and 2016 and the need to develop more effective and targeted tools to tackle the heightened risks and identify networks of financial support to terrorists.

In the awareness that EU FIUs greatly differ from each other in, i.a., their nature, independence status, organization, powers available, it was also felt that difficulties in effective cooperation might have to be traced back, at least in part, to how FIUs are structured and organized domestically.

Against this background, the EU FIUs' Platform launched at the end of 2015 a project aimed at mapping out existing shortcomings in FIUs activities and cooperation, specifically by understanding their nature and root causes. This "Mapping Exercise and Gap Analysis on FIUs' powers and obstacles for obtaining and exchanging information" (hereinafter: "Mapping Exercise") would, at the same time, assist FIUs in improving their cooperation, facilitate the implementation of the EU legislation, identify areas where further initiatives are needed to remove obstacles or remedy existing deficiencies[1].

The Mapping Exercise has been recalled and endorsed by the ECOFIN Council that, in the wake of terrorist attacks in Europe in 2015 and 2016 has encouraged "FIUs to accelerate their mapping exercise and, depending on the results of this exercise", has invited the Commission "to consider appropriate measures to tackle any obstacles to effective cooperation and information exchange"[2].

The Mapping Exercise is also consistently referenced in the Commission "Action Plan to strengthen the fight against terrorist financing[3]: "A mapping exercise is being conducted within the FIU 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"[4]; "depending on the results of this mapping exercise, the Commission will decide on whether and which kind of measures are necessary to address differences in the organisational status of the FIUs and tackle any obstacles to effective cooperation and information exchange". In fact, among the initiatives devised to implement the Action Plan on this point feature the adoption of regulatory initiatives aimed at "reinforcing the cooperation between FIUs through appropriate measures[5]".

The Mapping Exercise has been carried out by a dedicated Team led by the Italian FIU (Unità di Informazione Finanziaria per l'Italia - UIF) and comprised of 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)[6].

A Concept Note outlining the scope and objectives of the Mapping Exercise was discussed and approved by the EU FIUs' Platform in February 2016. A Survey was then launched to gather information from FIUs. This was based on a Questionnaire structure into nine thematic areas, ranging from FIUs' domestic features to the capacity to engage in FIU-to-FIU cooperation in its various forms and comprising 290 questions. Responses have been received from all 28 EU FIUs. Some of the feedback received was not complete or unclear and a number of follow-up questions

[1] This initiative is also consistent with, and fits well into, the conclusions and indications in the European Agenda on Security (COM(2015) 185) which, while recalling the importance of the new EU AML/CFT legislation and of its implementation for facilitating "the effective exchange of information between Financial Intelligence Units", has stressed the necessity "to align and reinforce the powers of FIUs", recognizing that "differences in their roles hinder cooperation and information exchange".

[2] See the "Council Conclusion on the fight against the financing of terrorism" of 12 February 2016.

[3] COM(2016 50.

[4] The Action Plan also specifically focuses on the need to enhance FIUs' operations and cooperation: "The Commission will also further look at means to support joint analysis of cross-border cases by FIUs and solutions to enhance the level of financial intelligence. As currently discussed at international level, the FIUs may also need to evolve from a suspicions-based disclosure system to a more intelligence-based disclosure system".

[5] These are scheduled for the second quarter of 2017.

[6] The FIU of the UK (National Criminal Agency – NCA) has also contributed to the Project in its initial phase.

have been addressed to respondents in the review phase. A wealth of good quality information has thus been gathered.

Based on the analysis of the material collected (and of other available information sources, such FATF or MONEYVAL Mutual Evaluation Reports), a template report has then been presented to the Platform in June 2016 followed by a complete drat report discussed by the Platform in September. Based on comments received and further analysis, a revised draft report has been made available to Platform Members at the beginning of November 2016. A final report, which takes account of additional inputs and comments, has been discussed and approved by the Platform in December.

2. Mandate, scope and objectives

The mandate received from the EU FIUs' Platform to conduct this exercise is particularly broad and involves aspects related to both the FIUs' domestic features and activities and cooperation with foreign counterparts. The mapping, in fact, should include: "a) the organization, powers and sources of information; b) the powers of FIUs in obtaining, exchanging information and use of all the relevant information (including the capacity to exercise domestic powers to respond to foreign requests); c) obstacles in obtaining information from obliged entities, exchanging/sharing information between FIUs, and use of information; d) root causes and possible solutions (enforcement of existing rules, administrative arrangements, new regulatory measures)".

Based on this ample mandate, the Mapping Exercise has not only looked into FIUs' cooperation, its features and deficiencies; prior to that, it has focused on domestic aspects and national arrangements concerning the FIUs' organization, independence, powers, information, in the assumption (which has been confirmed by the findings) that these aspects deeply influence the capacity of FIUs to engage in effective cooperation and that, therefore, they need to be considered to take stock of FIUs' activities and to identify existing obstacles. The analysis of the information gathered through the Survey has been conducted along two complementary axes.

Differences among EU FIUs have been explored and have been found to be particularly significant under all relevant respects (nature, organization, powers, information available or accessible, etc.). Under this "horizontal" analysis the issue has been discussed of whether the flexibility allowed by the Directive (particularly on domestic aspects) and the consequent diversity of approaches are conducive to good cooperation among FIUs. Under a different "vertical" perspective, the analysis has focused on the alignment with EU provisions, with the aim of coming up with a general overview of how and to what extent FIUs (or Member States) comply with these provisions. The findings on this point also raise several concerns as the legal framework relevant for FIUs at the national level has been found not yet in line with the fourth Directive (which is understandable, given that the deadline for transposition is 26 June 2017) but also non-compliant with provisions of the previous third Directive (as well as with the 2012 FATF Recommendations).

Specifically as regards the legal framework, it is important to consider that, while the Mapping Exercise has been largely based on the consideration of the provisions of the fourth Directive, the process for its transposition is still ongoing at national level. It is also necessary to recall that a Proposal for a new directive amending the fourth Directive was presented by the Commission on July 5th 2016[7] and was under negotiation at the time when the Survey was conducted and the Report drafted. It is reasonable to assume that national regimes and EU FIUs' practices depending on them will change when the implementation process will be complete. Nonetheless, it is important to flag

[7] COM(2016) 450.

that many of the shortcomings identified may not be solved simply through the transposition of the new EU provisions, for two concurrent reasons. First of all, in some areas national regimes applicable to the FIU do not even conform to the previous third AML/CFT Directive, which raises doubts as to the capacity to address these problems through the current implementation process. Secondly, several areas of concern have been identified in domestic aspects of FIUs' functioning, which do not fall into the scope of the fourth Directive and where significant discrepancies exist among national approaches.

Also based on these considerations, the Survey tries to flag cases where, besides implementation of existing EU provisions, a better convergence of domestic approaches should be fostered through more detailed and uniform rules at the EU level. The Survey also highlights cases where guidance or best practices could be identified and shared with a view to improve the level of convergence, which would benefit both FIUs' effectiveness in performing domestic functions and their capacity to provide adequate cooperation.

As regards particularly the aspects related to FIU-to-FIU cooperation, the scope of the Survey and of the Report is specifically focused on, and limited to, the capacity of EU FIUs to cooperate among themselves, which is precisely the scope covered by the EU legislation: neither the Directive nor the Mapping Exercise deal with international cooperation overall, between EU FIUs and FIUs from third countries. While the Directive is to a large extent consistent with global standards issued in this matter by the FATF and the Egmont Group of Financial Intelligence Units and it is expected that many of the findings and conclusions in the Report could be easily extended to FIUs' international cooperation as a whole, the EU framework has also several specificities. It is necessary, therefore, to bear in mind that, as often explicitly recalled in the Report, the analysis has been conducted specifically on EU FIUs' intra-EU cooperation and does not cover the external dimension of cooperation between EU FIUs and counterparts from third countries (as the Directive does not apply to that domain).

The Mapping Exercise, in line with the mandate conferred by the Platform, aims essentially at three main interconnected objectives: map existing shortcomings in EU FIUs' features, activities and cooperation; identify their root causes; devise possible ways to address the problems identified, thus providing inputs for policy makers (national and EU) and practitioners.. Specifically as regards the solutions that the report tries to set out, they can be schematically grouped in three categories: better FIUs' practices, to the extent permitted by the existing legal framework; better national transposition of EU provisions (where shortcomings or constraints have been identified in national legal frameworks); initiatives, of a regulatory or other nature, to be undertaken at the EU level (in cases where problems may be rooted in unclear insufficiently detailed EU provisions or where more convergent national approaches are needed).

Also due to its ample spectrum, the Report, while directly outlining possible measures or initiatives that can be undertaken where this appears feasible in light of the evidence gathered and the nature of the issue at stake, often flags areas where further research or analysis may be needed[8]. These are cases where the EU FIUs' Platform could consider planning future targeted work through dedicated projects.

[8] For example, on differences regarding suspicious-based and threshold-based disclosures, the identification of good practices on their types, structure and content and the definition of a common template; or on the indication of "financial", "administrative" and "law enforcement" information sources that should be available to FIUs for analysis and cooperation purposes.

3. Methodology

The Mapping Exercise, as said, is largely based on the analysis of information gathered from EU FIUs through an ad-hoc Survey and from other reliable sources. This Survey and the analysis have been conducted under two main assumptions that have directly informed the methodology underpinning the Exercise.

Differently from similar exercises conducted, within the EU or in other fora, on characteristics and deficiencies of FIUs' cooperation, the focus has been specifically put on domestic aspects, as previously mentioned. In fact, the capacity to provide cooperation has been considered and analysed as strictly correlated with the features of EU FIUs' concerning, i.a., their nature, independence status, organization, information available, powers exercisable, functions. The underlying assumption is that the FIUs' capacity to provide cooperation cannot but strictly depend on the FIUs' own characteristics, as determined at national level. The ability to exchange information and provide cooperation, under the multiple forms foreseen by the EU legislation, should not be seen in isolation but should be considered in light of FIUs' domestic features.

This approach has brought interesting results. The Survey, and the associated analysis, has highlighted not only that EU FIUs are significantly different from each other but also that, contrary to the approach taken by the Directive, these differences bear significant effects on the nature of the functions carried out (particularly "analysis") as well as on the capacity to access and use information. The same differences directly and deeply affect the EU FIUs' capacity to provide cooperation. As inherently and directly dependent on domestic conditions, it is found that cooperation is particularly influenced by factors such as the nature of the FIU, its relations with the institution where it is located, its status of independence, the specialised nature of its analytical functions as distinct from investigative activities.

While these considerations seem hardly surprising, as a matter of fact the approach usually taken by EU legislation and policy, as well as by other researches and analyses on the same matters, has been one where FIUs' cooperation has been treated as an independent variable. Considerable efforts have been dedicated to improve FIUs' cooperation but these have mostly overlooked the importance to focus also on domestic FIUs' features and consider the consequences of outstanding differences in nature and capacity. In fact, the EU (as well the international) approach to FIUs' regulation rests on an assumption that maximum flexibility should be maintained on domestic FIUs' features, under the condition that this should not go to the detriment of international cooperation. The analysis conducted shows that this assumption is difficult to maintain as the former influences the latter; the objective of ensuring good cooperation cannot be fulfilled in isolation and, most importantly, cannot be achieved in a landscape where FIUs are so diverse under several important respects.

This conclusion is important as it signals the important policy consideration that measures and initiatives aimed at improving the FIUs' capacity to cooperate and remove existing obstacles should not only focus on cooperation per se (e.g. the external dimension of inter-FIU relations) but should focus also on how FIUs are configured and organised and on how they function as independent and specialised agencies.

A second important element of the methodology underpinning this exercise should be recalled. As regards specifically the identification of limitations or obstacles obstructing FIU-to-FIU cooperation, the Survey is based on two different and complementary approaches. On the one hand, a comprehensive fact-finding exercise has been conducted on all elements pertaining to FIUs'

characteristics, information available, powers, functions, cooperation[9] These elements have been considered with the highest level of details possible to identify, at the same time, most prominent differences among FIUs as well as any other determinant that can influence the cooperation among them. Under a "building block" approach, the analysis has been focused on aspects concerning the organization, the independence status, the information available, the functions performed with a view to then understand how these aspects (and the existing differences) affect the capacity to provide cooperation and the extent to which this can be lent.

Again unsurprisingly, the mapping has allowed to highlight how limitations in information and powers available domestically, as well as issues surrounding the nature of the "analysis" function and the capacity to keep this, and the associated cooperation, distinct from law enforcement activities, has a direct bearing on FIU-to-FIU information sharing. This also provides arguments in support of more convergent domestic transposition of EU rules and, at the same time, of more detailed provisions at the EU level.

On the other hand, this "bottom-up" approach, whereby conclusions on FIUs' cooperation are drawn from information and analysis on discrete and detailed aspects making up the FIUs' inner workings and capacity to cooperate, has been complemented with a survey of most prominent obstacles or problems that EU FIUs encounter in their cooperation, based on a simple series of direct information and feedback gathered from respondents on this point[10].

This different, "top-down" approach has the twofold purpose of completing the mapping with any possible additional evidence of outstanding problems, and provide a tool to "back test" the analysis carried out and the consistency and robustness of its results. The two approaches (the bottom-up analysis and the top-down direct survey) have given convergent outcomes. The issues and problems identified through the detailed analysis conducted correspond to a large extent to those reported by respondents. In other words, the outcomes of the analysis find resonance with the feedback provided by EU FIUs on problems encountered in their daily practice of reciprocal cooperation[11].

In addition, of course, the analysis based on discrete elements concerning FIUs' features and activities allow to reflect on the possible root causes of the identified weaknesses or shortcomings and to formulate conclusions on possible measures or initiatives to address them.

4. Structure of the report

The Report consists of nine Chapters. EU FIUs' domestic status and organization is first described, recalling the distribution among different institutional "models", the tasks carried in addition to the FIUs' "core" function (receipt, analysis, dissemination, cooperation), the resources available and some essential features of the internal governance (Chapter 1). The analysis focused then on the autonomy and independence status of EU FIUs, discussing separately the capacity to carry out their functions in an independent manner and the extent to which independence is translated into

[9] These matters are dealt with in Chapters 1 to 8 of the Report.

[10] This survey is reflected in Chapter 9 of the Report.

[11] It is important to flag, though, one important circumstance. In responding to the detailed questions concerning domestic features and their own capacity to engage in cooperation, EU FIUs have provided information on themselves and have described (according to their own information and perception) how they work and perform domestically and in relations with their foreign counterparts. On the contrary, in responding to the section of the Survey on obstacles encountered in FIU-to-FIU cooperation, respondents have highlighted deficiencies referred to other FIUs or to the relations with them, that is problems caused by defective or inadequate practices put in place by foreign counterparts. Bearing in mind this difference in perspective is essential to properly understand the Survey and reconcile the outcomes in different sections.

organizational and management aspects; attention is also paid to the links with parent organizations and to how these links can affect the FIUs' autonomy (Chapter 2). A specific section is dedicated to the information that FIUs have available: that received through suspicious-based or threshold-based disclosures and that obtainable through access to "financial", "administrative" and "law enforcement" sources, including databases on bank accounts and on beneficial owners (Chapter 3). A detailed analysis follows on the EU FIUs' capacity to obtain information from obliged entities (Chapter 4). Domestic functions are then described and analysed, highlighting in particular existing differences as regards the "analysis" and the FIUs' capacity to apply a "selective" approach to processing and disseminating information, also through IT tools (Chapter 5). An ample survey follows on FIU-to-FIU cooperation; all relevant aspects are covered, ranging from the general capacity to provide information, cases for refusal, completeness of the information shared, the capacity to use domestic powers on behalf of foreign counterparts, innovative forms of cooperation (e.g. on cross-border disclosures and joint analysis), the capacity and limitations in providing the consent for further use or dissemination of the information exchanged (Chapter 6). "Diagonal cooperation", that is the exchange of information between FIUs and different authorities in other EU Countries, is dealt with separately (Chapter 7). Data protection, confidentiality and security safeguards are also discussed as regards the information processed throughout the FIUs' work cycle, from domestic receipt to FIU-to-FIU sharing (Chapter 8). Finally the feedback gathered from EU FIUs on main problems encountered in reciprocal cooperation is collected and discussed (Chapter 9).

Boxes are used throughout the report to highlight particular information, findings or conclusions. White boxes highlight elements taken from responses to the Survey, whenever these appear useful to support the description or analysis of particular aspects with factual information or example. Grey boxes, on the other hand, contain considerations on main findings for each topic dealt with, references to root causes, conclusions on initiatives or measures that could be taken. In some cases, broader conclusions on specific topics have been included in dedicated paragraphs, where this has appeared more conducive to clarity and ease of reading.

December 2016

EXECUTIVE SUMMARY

1. FIUs' domestic status and organization

Institutional setting - Nature of the FIU and organisation where it is located

Although with many nuances that make each national solution unique in its specificities, the EU FIUs can be grouped under three sufficiently homogenous "models", as regards their institutional nature and organization: administrative, law enforcement (or judicial) and "hybrid".

It is important to underscore that the identification of these different institutional models is purely conventional and the distribution of EU FIUs among them is somewhat arbitrary. Each FIU maintains in fact its distinctive peculiarities, even within each category. It is also necessary to bear in mind that, against a background of broad flexibility allowed by the Directive, EU FIUs are all different from each other, particularly as regards their status or nature, the internal organization and governance, the composition of the staff. Although some commonalities can certainly be identified, each Member State has defined a unique and peculiar "blend" for its FIU. This results in a very varied and diversified "landscape".

EU FIUs are set up within bigger host organisations, which in most cases provide the logistics, the budget and other resources. FIUs do not normally have their own legal personality, as they are part of the bigger legal person or public entity where they are located.

Administrative, law enforcement and "hybrid" FIUs

Twelve EU FIUs have indicated that they have an administrative nature. These FIUs are located, often as specialised and autonomous units or departments, into the ministries of Finance, Justice or Interior. Others are embedded into the Central Bank or a supervisory authority.

Eleven respondents have indicated that they are organised under a law enforcement "model". These FIUs are established in, or are part of, the respective national criminal police offices, agencies or services. They appear to be set up at different levels of the internal organisation, either as separate units (with their own forms of governance) or as internal offices of law enforcement structures competent for fighting economic crimes or other serious crimes.

Five respondents have described themselves as having a "hybrid" nature, due to the combined presence of administrative and police elements. These FIUs are mostly located in national police offices or in the office of the attorney general or of the prosecutor, are separate from operational police or judicial units and are specifically dedicated to the analysis of suspicious transactions. The staff of hybrid FIUs often includes, in addition to law enforcement officers, analysts from other, non-police, organisations.

Impacts on the functions

The replies to the Survey seems to suggest that, far from being neutral, the nature and status of FIUs have far-reaching consequences on their functions and powers, as well as on domestic and international activities. The nature and institutional setting of the FIU can specifically influence the nature of its function of "analysis" of suspicious money laundering and terrorist financing cases. This function is not defined or described in details in the Directive and, in lack of a common notion towards which they can converge, FIUs conduct activities which, although equally labelled as "analysis", differ considerably in, i.a., scope, extent, information used, outputs and objectives.

Police-type FIUs tend, in general, to carry out investigations based on STR/SAR material, thus merging analysis and law enforcement tasks into a unique activity. Cases where the distinction between analysis and investigation is blurred and the two are commingled, with the former being absorbed in the latter, bring a number of interconnected consequences, particularly on the type and range of information available to the FIU (either received through disclosures or obtainable), the nature and objectives of the activities carried out, the capacity to provide information and cooperation to foreign counterparts.

The objective of making FIUs' activities and cooperation more effective and uniform cannot be achieved without reflecting on the need for more convergence among national approaches to FIUs' domestic status and features. The Survey, in fact, suggests that improvements in FIUs' capacity to cooperate and an increased convergence towards homogeneous functions would require a higher level of uniformity in FIUs' domestic features, together with a corresponding reduction of the flexibility currently allowed by the Directive.

Conclusions on FIUs' status and organization

The current approach to FIUs' regulation in EU provisions is based on minimum or no harmonisation of domestic institutional and organizational features and a focus instead on the functions that FIUs have to perform and on the powers and information that should be available for that purpose. This has resulted in a very diversified "landscape" of national solutions, whereby FIUs are all set up under different arrangements even within the three identified "models" of "administrative", "law enforcement" and "hybrid" units, and are organised along different institutional features. In addition, the provisions in the fourth Directive about FIUs' necessary functions, information and powers lack details and, as a result, EU FIUs have different mandates and carry out different activities, contrary perhaps to the objectives pursued by the Directive.

For these reasons, the current paradigm underpinning the EU regulatory framework for FIUs, that is FIUs' nature and organizational features may vary provided that the same functions are exercised and sufficient information and powers are made available, may prove not to be correct. In fact, the extent of the flexibility allowed to Member States on the former aspects (nature and organizational features) influences the latter (functions, information and powers) and determines divergent approaches across Member States, with undesired effects also on FIU-to-FIU cooperation. Consideration should therefore be given to:

- setting minimum indications on domestic FIUs' features and organization, constraining in part the current excessive flexibility with a view to ensuring more convergence on functions and powers which is also conducive to better FIU-to-FIU cooperation[12];
- drafting more detailed provisions on the characteristics of FIUs' functions, notably as regards "analysis" as distinct from law enforcement activities, the underlying objectives and the information that FIUs should be able to receive or obtain to pursue them and to entertain effective cooperation.

[12] On this point, it is important to recall the Commission "Action Plan to strengthen the fight against terrorism financing", adopted in February 2016 (COM(2016)50), which specifically recall that, "depending on the results of the mapping exercise, the Commission will decide on whether and which kind of measures are necessary to address differences in the organizational status of the FIUs".

Additional functions carried out by FIUs

In addition to the FIU "core" tasks (receipt, analysis, dissemination, international cooperation), FIUs can of course be entrusted with additional functions, based on domestic legislation and arrangements. The majority of respondents to the Survey have indicated that they indeed perform a considerable variety of additional tasks. These range from law enforcement to supervisory activities, from regulatory to coordination functions in AML/CFT related areas. FIUs may also play a role in the implementation of targeted financial sanctions and in providing training to the private sector or to public partners.

It is necessary that an appropriate separation is ensured between the functions carried out by FIUs as such (that is, those making up their very definition: receipt, analysis, dissemination, plus international cooperation) and the other, additional tasks assigned to them. This separation should be implemented both through appropriate organizational settings and by ensuring that the information collected and processed in the exercise of the FIU's functions is kept confidential and is not unduly used for different purposes.

Human resources

Whilst the most staffed FIU has reported 300 employees and the least staffed has indicated 13 persons, the average amount of human resources available to EU FIUs is 58. The majority of FIUs are below this average, with fourteen respondents reporting up to 30 employees. Three medium-sized FIUs have between 58 and 100 members of staff, while the four most endowed FIUs have in excess of 100 staff.

For the majority of respondents, the biggest portion of the human resources available is dedicated to the performance of core functions associated with the receipt of STRs/SARs, analysis, dissemination and international cooperation. However, significant amounts of resources are also allocated to other tasks.

Financial resources

Only less than half of the EU FIUs have indicated that they dispose of an autonomous budget, that is an amount of funds assigned specifically (and exclusively) to them for expense coverage and managed autonomously. Seventeen respondents have in fact indicated that, being part of bigger organisations, they draw the needed financial resources from those organisations, within the budget of these latters which is normally determined by the Parliament, in case of ministries, or by ministries, in case of separate organisations such as police bodies or judicial offices.

Lack of an autonomous budget

Problems may arise, in these circumstances, if the overall budget of the host organisation is limited, in such a way as it is not sufficient to support properly the needs of the FIU.

The budget of large and complex organisations has of course to support multiple and diverse activities and entities within the general area of competence. As a consequence, the expenses needed and requested by the FIU may not feature sufficiently high in the overall list of priorities. In these cases of conflicting or overlapping priorities, the objective of securing the adequate functioning of the FIU could be postponed with respect to other objectives that are considered more pressing, to the detriment of both the effective operations of the FIU and of its independent and autonomous management.

While political considerations in spending matters are normally fully legitimate, when they impact on the functioning of the FIU the capacity of the latter to function independently may be affected. Especially in cases of significant cuts in spending, the FIU's effectiveness can be affected too.

Autonomous budget
As regards the eleven respondents that have indicated that they dispose of autonomous budgets, for whose spending they are also responsible, the amount of available resources vary considerably, ranging between a minimum of 600.000 EUR and a maximum of above 14 million EUR on a yearly basis. The adequacy of these figures could of course only be assessed taking account of factors such as the dimension of the interested FIUs (which is clearly an important determinant for spending needs and also varies considerably across the EU), the spectrum and types of the tasks assigned, the magnitude of the workload and volume of the activities carried out.

"Mixed" approaches
In contrast to FIUs that either have dedicated budgets or can only obtain resources from the parent organization, some respondents have indicated that they operate under a mixed approach: while the bulk of the expenses is sustained by the host organization through its budget, these FIUs are also endowed with a (relatively limited) amount of financial resources which they can spend autonomously for particular purposes.

IT resources
The majority of the respondent FIUs believe they possess adequate IT tools dedicated to supporting the receipt, analysis, dissemination and international cooperation. In most cases, FIUs have developed in-house or ad-hoc IT systems in order to carry out their functions. A number of FIUs, instead, are using, or are planning to adopt, IT products offered by external providers and adjusted to fit into their peculiar operational and procedural contexts. In general, a broader use of IT tools is indicated by respondents as a means to cope with the increasing workload by enhancing efficiency. The analysis has highlighted cases where IT tools are lacking and FIUs maintain paper-based working procedures, to the detriment of effective information processing and analysis.

Conclusions on resources
The fourth Directive considerably expands FIUs' activities and related powers and at the same time, increases the complexity of such activities. This is particularly true in the area of FIU-to-FIU cooperation, where several innovations have been introduced. For example, EU FIUs are now required to make use of available domestic powers (that in turn have been expanded) to respond to foreign requests and to forward to interested foreign counterparts STRs/SARs that "concern another member State". As consistently indicated by respondents, these innovations bring about an increase in activities which are likely to put considerable strains on FIUs' resources. This goes together with a workload that is constantly increasing, particularly as regards the volumes of STRs/SARs received, the need to perform operational and strategic analysis as two different, though connected, functions; the approach to operational analysis based on the capacity to consider all information and then selectively single out cases and data deserving further follow-up, the demands associated with different forms of domestic cooperation[13].
Concerns are voiced by EU FIUs as to the FIUs' continued capacity to face expected developments in the absence of an increase in available resources. In this context, faced with an expanded mandate and a higher level of complexity of their "core" functions of receipt, analysis, dissemination and international cooperation, FIUs (and Member States) should also reflect on few additional considerations.

- Make efforts to recast the FIUs' tasks with a view to concentrate resources on the effective performance of core activities as mandated by the Directive. As flagged by some respondents, this objective should be achieved also by improving the efficiency of working procedures and developing appropriate IT tools in their support.

[13] Although this is not explicitly recalled in responses to the Survey, FIUs' role has been expanded particularly as a consequence of heightened terrorism threats.

- Reinforce FIUs' operational independence and autonomy, conducive to achieving a higher level of effectiveness. In particular, FIUs should dispose of resources which should be commensurate with the organizational and operational needs and determined outside of undue political considerations.

Internal organization - Organs and structure

The internal organization of EU FIUs varies depending on the functions carried out and on their size. In some Countries FIUs are set up as relatively small units with very simple structures. In other cases, FIUs entrusted with multiple tasks, or facing bigger workloads, have more complex and articulated internal organizations, commensurate with the activities performed.

When the staff working for the FIU comes from different organisations, this may pose issues of, i.a., confidentiality, direction, homogeneity of working methods. In these instances it is important that the external staff responds in full to the FIU's hierarchy, without having to report to the organization of origin, and is bound by the latter's internal procedures. Organisations which have a federal configuration should ensure that all decision making processes are kept centralised and that procedures and information are kept within the FIU.

Appointment and removal of the Head of the FIU

The appointment and removal of the FIUs' Head is of course a cornerstone of the FIUs' organization and status of independence. Differences among EU FIUs in procedures and competent authorities depend crucially on the nature of the FIU and the relations with the organisation within which it is located.

The Head of administrative and "hybrid" FIUs is generally appointed by the Head of the organisation within which the FIU is located or by the Government or other national competent authority (e.g. Ministry of Finance, the Attorney General, the King, etc.). In these latter cases, the decision is often taken upon a proposal by the Head of the organisation within which the FIU is located. In some cases the appointment is subject to ad-hoc hiring procedures or public calls, based on applications by candidates and the assessment of their merit.

The Head of law enforcement/judicial FIUs is normally appointed by the Head of the national police, the Minister of Interior or by the Public Prosecutor's office.

As regards the duration of the mandate, Heads of FIU are frequently appointed for a pre-determined period of time (3-5 years), frequently renewable once. In a few cases, no particular duration is set.

Accountability

FIUs' accountability should be improved. More information and statistics need to be produced and made available by FIUs on their activities and the relevant outcomes. This set of information should be forwarded to partner authorities and to competent policy makers. It should also be disclosed to the private sector and to the public in general. Appropriate consideration should be given to introducing minimum common requirements at the EU level to enhance EU FIUs' accountability in a sufficiently uniform framework.

2. Operational autonomy and independence

The requirement of operational independence and autonomy has two aspects: the capacity of the FIU to take autonomous decisions and responsibilities in performing its "core" functions; the availability of sufficient resources and capacity to manage these resources and to organise itself independently to pursue its functions by taking autonomous decisions. While the responses to the Survey provide a general positive feedback on EU FIUs' capacity to take decisions without influence from third parties, further analysis shows that several constraints are in place.

Autonomy in the receipt of STRs/SARs

The FIUs' independence in receiving STRs/SARs may be translated into two main elements: a) the capacity of FIUs to obtain these disclosures directly, that is from the reporting entities themselves and without the interposition of third parties; b) the capacity of FIUs to receive the disclosures exclusively, i.e. without these being submitted by reporting entities also to other agencies.

Interposition of other bodies

In accordance with article 34(1) of the Directive in relation to certain obliged professionals[14], Member States have the possibility to designate an appropriate self-regulatory body as the authority to be informed in the first place, instead of the FIU. Reponses seem to show that only few Member States and FIUs have availed themselves of this option. Also, as mandated by the Directive, the interposed self-regulatory organizations that are allowed to receive the disclosures in the first place are normally obliged to forward them to the FIU ("promptly") and are prevented from setting them aside, thus not informing the FIU about reported cases, or from even filtering out information included in the disclosures.

It appears, however, that there are cases where the interposed self-regulatory organizations are entitled to exercise some evaluation on the disclosures received and apply some filters on their content. To the extent that this evaluation entails discretion, which can translate into STRs not being (entirely) forwarded to the FIU, this system may raise issues of misalignments with the requirements in the Directive on this point with impacts on, i.a., the FIU's independence in the receipt function.

The FIU as the only recipient of STRs/SARs – Exclusive and multiple reporting

Responses also show that there are cases where, although the FIU receives the STRs/SARs from reporting entities, these are at the same time required to forward the same disclosures also to other domestic bodies (for example, fiscal authorities or law enforcement agencies or prosecutors).

Systems where dual or multiple reporting systems are in place, besides not being foreseen by the Directive, raise several concerns. STRs/SARs information, collected for the purpose of allowing the analysis by the FIU on potential money laundering or terrorist financing cases, is used also for other purposes and by agencies other than the FIU, before and regardless of the FIU's dissemination. In parallel with the FIU's analysis, investigations may be started on the same facts and based on the same information, which certainly may bring peculiar challenges in terms of coordination of actions by different agencies and consistency in findings and results.

In cases where the disclosures are sent at the same time to the FIU and to police agencies or prosecutors, the distinction between analysis and investigations becomes blurred and the former would be made subject to the latter, with possible implications on FIUs' independence and quality analysis. Direct upfront disclosure to multiple agencies may prevent the FIUs from adding value through analysis and subsequent dissemination.

Parallel direct disclosure to multiple agencies deprives the FIU of its role of bringing added value to the case through analysis, "overrides" the dissemination function and brings inherent coordination challenges, as each involved recipient will consider the information on its own and for its purposes.

While STRs/SARs are designed to trigger analyses by FIUs on money laundering and terrorist financing cases, their direct transmission to other agencies for pursuing different purposes (like tax violations), does not appear in line with this limitation. Concerns can also be raised in terms of adequate confidentiality and integrity of these sensitive disclosures.

Reinforced or clearer provisions at the EU level may be considered in order to ensure that, in each Country, the FIU should be the only recipient of STRs/SARs.

[14] These are: lawyers, auditors, external accountants, tax advisors, notaries, real estate agents.

Autonomy in the analysis. Inception – Triggers and priorities

Responses to the Survey indicate that FIUs decide autonomously when an analysis should be started. On this aspect, however, account needs to be taken of existing forms of influence on FIUs' determinations to conduct analysis, which can impact on the independence condition, exercised by external parties, notably by the organization where the FIU is located or police agencies or prosecutors in the context of law enforcement activities.

An important consideration for FIUs when initiating analysis is to establish the level of priority of the cases that should be considered. This is essential especially when there is a sheer volume of information to process and resources have to be deployed appropriately. This is also important because, under the Directive, the analytical function has now an element of "selectivity" which requires FIUs to consider all available information but, at the same time, to focus on relevant cases.

Appropriate independence and autonomy should be exercised by FIUs in deciding about conflicting priorities taking account exclusively of the relative importance of the cases under consideration.

The lack of sufficient resources to cope with increasing workloads, besides forcing FIUs to sharpen the capacity to identify and solve conflicting priorities, may impact on FIUs' operational independence and, at the same time, on their operational effectiveness.

The analytical process

After the inception phase, FIUs should also carry out the analytical process in an independent manner. This process should be driven by FIU's considerations about the features of the cases under analysis, their complexity and level of priority, the objective to produce a useful outcome based on actionable intelligence for subsequent investigations or prosecutions. In this context, for example, FIUs should be able to decide freely which information should be obtained and whether other domestic authorities should be approached with requests or foreign FIUs contacted for sharing information on relevant cross-border elements. Responses seem to indicate that EU FIUs are generally capable of managing and shaping the analytical process taking autonomous decisions.

Some FIUs (embedded in police organizations) indicate that external staff from law enforcement agencies can be associated to the analytical activities. The involvement of external staff into FIUs' analysis provides opportunities to exploit synergies with other agencies, leverage on a broader set of skills in complex cases, maximize the use of resources and possibly compensate for lack of FIUs' staff especially in cases of increasing workload. At the same time, in the absence of adequate safeguards and controls, the access by external staff may cause STR/SAR information to be unduly shared or circulated and used for purposes other than analysis by the FIU. The continuity in the use of FIUs' resources may also be affected, due to turnover of analysts. Potential impacts on the operational independence of the FIU should also not be underestimated; systematic or excessive dependence on external staff may be an indicator of insufficient capacity of the FIU's to discharge its core functions. Also, relying on, and employing, external resources might affect the FIU's capacity to manage its tasks autonomously and under appropriate confidentiality requirements. Seconded analysts, whilst not fully integrated into the FIU's organization, may remain subject to direction by the organization of origin. This risk may be heightened for FIUs that are embedded as an integral part of the police agency that seconds the analysts.

These concerns should be mitigated through appropriate measures.

Conclusion of analysis

Autonomous decisions should also be taken by FIUs concerning the conclusion of the analytical process, particularly as regards the stage at which the analyzed cases is considered ripe for the appropriate follow up.

The need for FIUs to take a selective approach on cases and on information has to be recalled in this perspective. Decisions have to be taken, in an independent manner, on the identification of cases which deserve an investigative follow-up, the assignment of motivated priorities to such cases, the selection of the intelligence developed through analysis capable to support ensuing investigations.

Responses seem to confirm that EU FIUs are generally in a position to decide autonomously when the analytical process is complete, all necessary intelligence has been developed and the case is ripe for the required follow-up. In any event, the FIUs' capacity to determine freely the conclusion of the analysis has to be considered together with possible conditions or constraints in the subsequent dissemination.

Autonomy in the dissemination

The requirement of FIUs' operational independence with regard to the dissemination has multiple dimensions and needs to be considered under different angles: the decision on whether or not a case should be disseminated (outside of cases of dissemination on request); the timing of dissemination; the information that should be forwarded.

Active dissemination vs. passive access to FIUs' databases

It is important to underscore that the dissemination function is based on an active role which should be played by the FIU: this has the responsibility to identify, through analysis, cases and information that need to be followed up in ensuing investigations or prosecutions and forward these cases and information to competent agencies. For these reasons, systems where FIUs' STR databases are passively accessed by domestic law enforcement agencies do not seem in compliance with the EU provisions on FIUs' dissemination, both as regards the features of this function (which implies active enrichment through analysis and appropriate selection of cases) and the FIU's independence in its exercise.

Independent decision to disseminate

Many respondents confirm that they take independent decisions on the outcome of their analyses and, accordingly, on whether the analysed cases should be disseminated, as they are indicative of money laundering or terrorist financing activities, or closed and set aside, as they turn out to be unfounded. The independence requirement lies in the FIU's capacity to determine whether the analysed cases are potentially linked to money laundering or terrorist financing and does not imply that, when it turns out that this is the case, the FIU can decide not to inform competent authorities for the necessary investigations or prosecutions.

Timing of dissemination

Independent decisions have to be taken by FIUs also on the timing of dissemination, which depends on when the analysis is considered complete and on the "readiness" of the case. Should other parties be able to "pull" information from the FIU before the analysis is complete and dissemination is spontaneously performed, this would amount to a limitation of the FIU's "ability to take autonomous decisions to disseminate". Cases of direct access to the FIU's STR/SAR database may fall into this scope.

Recipient competent authorities

FIUs also take determinations on which competent authority should be the recipient of each particular dissemination, depending on the nature and the expected follow-up of the underlying cases. The recipient of dissemination is normally identified among law enforcement agencies or prosecutors, also taking account of the possible existence of investigations or legal proceedings that may be ongoing.

In other instances, the FIU is obliged to disseminate cases and information to agencies that are specifically designated by the law. In such cases, the FIU may not be allowed to exercise any discretion and forward information to other competent agencies that, based on the nature of the case, the outcome of the analysis and possible existing investigations or prosecutions, may be best positioned to act upon the case.

Restrictions to the FIU's capacity to identify the recipient authorities, as those that, based on the nature of the case and the outcomes of the analysis, are in the best position to effectively pursue the necessary investigations or prosecutions, may result in limitations to both the effectiveness of the dissemination function and the FIU's independence in this particular respect.

Disseminated information

FIUs are not expected to forward all the information they receive or obtain. They should exercise their independent judgment in selecting relevant information to disseminate, having regard to the outcome of the analysis and to the need to be "specific", thus facilitating ensuing investigations or prosecutions. Therefore, the requirement of independent dissemination has also another important dimension: the FIU should be able to establish, in light of the cases and the related analysis, the most appropriate set of information that should be included in the dissemination "package" to properly illustrate the intelligence produced and support the ensuing investigations.

Responses indicate that the disseminated information normally includes the disclosures received and the relevant intelligence gathered through the analysis. At the same time, FIUs report that they generally have the capacity to select the information to forward to competent authorities.

However, some FIUs are obliged by law to disseminate all received STRs/SARs, with their full content, with no possibility to set aside those disclosures or information which, based on the analysis, do not appear to be relevant or actionable. In these cases the "selection" element may be less developed or pronounced; together with limitations to the FIUs' independence, this implies that no filtering is applied.

Autonomy in receiving or accessing threshold-based disclosures

In most cases, threshold-based disclosures provided for by domestic legislations are received directly by the FIU. In these instances, as confirmed by respondents, FIUs can certainly use these disclosures for their own analytical purposes in full autonomy, with no need to obtain access through (or authorised by) third parties.

In other cases, threshold-based disclosures are forwarded by obliged entities to other competent recipient authorities. This typically happens for the declarations on physical cross-border transportations of cash, as foreseen by the Regulation (EC) n. 1889/2005.

While FIUs that receive disclosures directly have of course no difficulties in using their content any time it is needed, it is less clear from responses if the same level of autonomous use is available to FIUs that have to gain access to objective disclosures received and held by third parties.

Autonomous access to external sources of information

Responses to the Survey show that, although the access to external sources of information, including data held by other authorities and law enforcement data, is generally possible without impediments, FIUs are subject to limitations that may affect their capacity to obtain information in an independent manner. It appears that in some instances the access to external sources can be made subject to conditions and discretional evaluation by the agency holding the information sought which go beyond mere authentication formalities.

FIUs may be prevented from freely accessing external sources of information when investigations or legal proceedings are underway on the same cases on in relation to the same information. These are instances where the FIU, rather than independently accessing relevant sources based on its information needs, is subject to an authorization or an "agreement" with competent agencies.

Moreover, cases of indirect access are particular widespread and this, coupled with the above mentioned conditions, can also affect the FIUs' capacity to freely and rapidly obtain the information needed for analysis or international cooperation.

Autonomous capacity to request and obtain information from obliged entities

Responses generally highlight that the FIUs' power to obtain information from obliged entities can be exercised under no particular conditions or filters and without depending on third parties' authorisation. Despite a general positive feedback, responses also highlight that, in some cases, conditions and limitations apply to the FIUs' capacity to obtain information from obliged entities.

The existence of investigations or legal proceedings on the same or related cases or information may inhibit the FIU's capacity to approach obliged entities. Moreover, some FIUs need a prior authorization from competent courts or prosecutors in order to be able to approach obliged entities with an enforceable request to receive information. Besides domestic analysis, conditions associated with the existence of investigations or a necessary prior authorization for obtaining information from obliged entities also affects the FIUs' capacity to provide information to foreign counterparts.

The requirement to subject the FIU's access to information held by obliged entities to a court or prosecutorial order seems to be rooted in the assumption that such access is a law enforcement measure that, as such, is not a natural prerogative for the FIU and should therefore be "validated" by competent investigative authorities. This assumption does not seem to find any support in the Directive which, on the contrary, maintains that FIUs should be able to obtain this information specifically in support of their analysis (and related FIU-to-FIU cooperation) which is distinct and independent from law enforcement activities.

It is hoped that forthcoming amendments to the EU provisions on this point will further clarify that FIUs should be directly and autonomously able to obtain information from obliged entities, thus requiring Member States to transpose this requirement into domestic laws without any undue conditions or limitations on the FIUs' capacity to approach obliged entities directly.

It is also important to recall that the capacity to request information is, for some FIUs, dependent on the existence of an STR/SAR previously reported to the FIU on the same case or subject.

Autonomy in cooperation with domestic authorities and other FIUs

EU FIUs indicate in their responses that they have the capacity to engage independently and exchange information with other domestic authorities with no need for authorizations from third parties. The same feedback is provided for the cooperation with other FIUs; "memoranda of understanding" can also be negotiated and signed by FIUs autonomously.

Against this general background, however, the EU FIUs' ability to engage independently in reciprocal cooperation continues to encounter limitations. These are related, for example, to a limited capacity to access and share particular types of information (e.g. that held by certain obliged entities, financial, administrative or law enforcement data), the need to obtain authorizations for providing certain information (particularly when investigations or legal proceedings are underway) and limitations in providing the consent for further use or dissemination of the information exchanged, still often dependent on the existence of investigations or legal proceedings.

Autonomous capacity to suspend or withhold consent to suspicious transactions at the request of another EU FIU

Some respondents point out that the capacity to postpone transactions on request by foreign FIUs has not yet been specifically implemented in national law, as this was only introduced by the fourth Directive. In some cases, while the FIU can take action to secure a postponement (also upon foreign requests), the decision to issue the necessary order falls under the competence of another authority.

Cases where the decision to postpone a transaction reported as suspicious to the FIU is taken by a different domestic authorities upon the FIU's initiative, as allowed by the Directive, may raise concerns under several respects. In general, although the postponement power is not formally vested in the FIU, whenever the suspension is not adopted by the competent authority, this would imply a limitation to the FIU's own assessment and discretion; as mentioned, especially if contrasting decisions by the competent authority are frequent, the FIU's status of independence may even be at stake.

Autonomy and independence in the FIUs' organisation

FIUs' effective operations and independent and autonomous functions depend critically on the availability of sufficient resources and on the capacity to manage these resources without undue influence or interference from third parties. Lack of resources would prevent FIUs from fulfilling their tasks, despite any formal independence that may be recognised. At the same time, having resources available but not being able to manage them autonomously would also directly affect the FIU's capacity to independently determine and pursue relevant priorities or even achieve set objectives.

Adequacy of resources

EU FIUs are under considerable operational pressure and their resources are reported to be under severe strain. They are faced with increased workloads, higher and more diversified types of information and additional, sometimes innovative tasks. This determines that available resources may be, or become, insufficient or inadequate, with potential consequences on the FIUs' capacity to remain effective in providing useful inputs to prevent and detect money laundering and terrorist financing cases and, as a consequence, to operate under appropriate independent conditions.

As flagged in several responses, EU FIUs demands for additional resources are often declined by competent authorities due to general budgetary constraints, as a consequence of deteriorated economic conditions.

National policy makers should ensure that FIUs' human and financial resources are adequately increased (in quantity and quality) to maintain effective and independent functioning. In this, the necessary level of priority should be recognised to the role of the FIU in the context of general public policy and expenditure choices. This is also essential to fulfil the condition established in article 32(3) of the fourth Directive which maintains that, of course taking account of evolving activities and the increasing workload, "Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks".

To properly cope with the increased volumes and complexity of FIUs' activities the implementation of suitable IT tools and working procedures is also essential. This not only fosters the efficient use of resources but is also conducive to the objective of FIUs being able to process big and diversified volumes of data maintaining the capacity to consider all information in an integrated manner, automate the analysis process and selectively focus on relevant cases.

IT-supported working procedures also reinforce FIUs' capacity to adopt independent decisions, both as regards the identification of priority areas where available resources should be deployed. The need to develop adequate working procedures, case management and analytical tools based on dedicated IT instruments in support of FIUs' activities, could be taken up at EU level, both by recognising relevant needs and existing practices and by requiring Member States and FIUs to work in this direction.

FIUs and Member States should be encouraged to make sure that, for FIUs that carry out multiple tasks, some of them additional to the core functions, a careful assessment of priorities is conducted to avoid that essential FIUs' functions are not compromised due to lack of resources as these have been distributed across a range of diversified activities.

Assignment and independent management of resources

Several constraints are reported and described by respondents as regards the FIUs' capacity to obtain the resources required and to manage them based on fully autonomous decisions. Some FIUs, although they depend upon external decisions, maintain a level of independence in setting resource needs, obtaining and managing resources. Other FIUs, instead, indicate that they have little or no control or influence over the assignment of resources, which is exclusively determined by the bigger organization where they are located. A reduced capacity to manage these resources is also frequently mentioned in responses.

A considerable number of FIUs point out that they are in no position to decide upon increases in staff or other resources. All these constraints are dependent on these decisions being reserved exclusively to the organisation where the FIU is embedded.
The concentration of all decision powers concerning the assignment and use of FIUs' resources within the parent organization may also imply that this organization not only decides whether staff should be deployed to the FIU, and to what extent, but can also withdraw or divert employees from the FIU and second them to other units in support of activities or projects carried out by these latter.
Although FIUs may maintain some capacity to put forward their needs, requests or proposals, the parent entity remains in charge of all essential management and organization determinations concerning specifically: a) the amount of resources assigned to the FIU (both human and financial); b) the acquisition of new resources, particularly through external recruitment or transfer from other units of the parent organization (as well as the attribution of additional budget); c) the promotion of staff or its appointment to particular positions within the FIU (although some respondents have signaled that they have some room for taking autonomous decisions on these particular aspects); d) the acquisition or development of IT tools in support of the FIU's activities; e) the internal organizational structure, for example through the setting up of internal units or their modification to take account of the evolving context.
The limited capacity of EU FIUs to take autonomous decisions on their resources and internal organization is thus a consequence of the particularly close link which binds FIUs to the organization where they are embedded. This entails significant limitations to the EU FIUs' autonomy and independence under this respect.
Against this background, it seems important that the implications of the requirements about "operational autonomy and independence" (only generally recalled in article 32(3) of the Directive) on the FIUs' capacity to manage resources and other aspects of their organization and functioning be properly identified and clarified. EU provisions or indications in this regard would allow to come to a common understanding of these organizational requirements and to ensure that adequate minimum conditions are implemented uniformly and consistently across Member States.
The current FATF standards on FIUs' autonomy and independence (in the Interpretive Note to Recommendation 29) could be reflected into the EU legal framework. Further details could be spelt out on how EU FIUs should be able to act independently on resources and other organizational matters, for example as regards the capacity to obtain adequate resources and manage these resources independently, including with respect to the host organization. These indications could include, for example, references to processes for recruitment of selected and high skilled staff specifically destined to the FIU. Furthermore, the need for a separate management of the FIU staff and resources with respect to those of the parent organization could be explicitly foreseen.

Links with external parties (host organization; law enforcement agencies and prosecutors)
The operational independence and autonomy requirements established by the Directive apply to FIUs vis-à-vis any third party. This scope includes also (and perhaps primarily) the relations with the host organization within which the FIU is located.
Responses to the Survey show that the requirement that FIUs should be able to take "autonomous decisions" on matters concerning the exercise of their functions and powers, or their resources and organization, is not properly implemented in situations where the FIU, being embedded in a bigger organization, is subject to hierarchical links with the latter.
Several FIUs inform that they are indeed subject to direction or decisions from higher staff belonging to the organization where they are located. Such hierarchical influence can be exercised either on the performance of the FIU's functions or on organizational matters. Based on the information gathered through the Survey, it appears that the exposure to hierarchical links and influence from the host organization depends crucially on the level of embedment of the FIU within such organization: limitations to the independence appear to be more significant for FIUs that are

embedded more "deeply" within the host organization (that is are located under the responsibility of other units, directorates or departments), as the level of autonomy decreases accordingly.
Equally, limitations to the FIUs' independence seem to arise in cases where, outside of ordinary national cooperation and coordination mechanisms, the FIU is in close relations with investigating or prosecuting bodies and can be ordered by these bodies to perform specific analysis or acquire particular information or are otherwise instructed on priorities to pursue[15].
Hierarchical links and powers may entail the capacity of staff from the host organization, or other outside staff, to access, or otherwise obtain, information held by the FIU concerning STRs/SARs, related analysis and international cooperation.
A better national implementation is needed to secure that the FIU is duly isolated, even within the host organization, from undue hierarchical links which may extend to organization and operations matters or translate into influence on activities or priorities. Dedicated indications at the EU level, for example through targeted amendments to the provision in the Directive, could explicitly set out a common requirement for Member States to ensure that FIUs maintain their autonomy and independence specifically with respect to the host organization where they may be embedded.
Similarly through better domestic implementation and targeted common rules at the EU level, an increased focus should be put on the confidentiality regime of the information held by the FIUs, as regards undue access or sharing with third parties outside the ordinary dissemination mechanisms, particularly with respect to the authority where the FIU may be located.

3. Information received, available and accessible to FIUs

Disclosures received on suspicious activities
As a consequence of the lack of detailed indications in the Directive on the "suspicious transactions" or "suspicious activities" reporting obligation, Member States have taken different approaches to the determination of triggering factors, structure and information content of this obligation. Different types of disclosures have been introduced, variably named "Suspicious Transaction Reports" (STRs), "Suspicious Activity Reports" (SARs) or "Unusual Transaction Reports" (UTRs). To differences in names correspond differences in nature, substance and content. Equally, relevant triggering factors vary significantly across countries, as the notion of "suspicion" is differently defined (and qualified by guidance or indicators). This has an impact also on the volumes and contents of disclosures received by EU FIUs.
In terms of scope and range of the information which should be included in suspicious transaction reports, these may vary depending on the existence of other disclosures that the same FIU receives or on the extent of the information powers the FIU can exercise to obtain additional information as needed for the analysis of the disclosures received.
While there is no evidence that the different information tools used in Member States are in all cases well balanced and result in FIUs having an adequate range of information available, differences in FIUs' capacity and powers are likely to affect the type and quality of the analyses performed by different FIUs and also their capacity to provide cooperation.

Nature and use of disclosures on suspicions: STRs, SARs, UTRs
Against the background of article 33 of the Directive, the approaches taken by Member States to defining "STRs" differ along essentially two axes: the nature of the disclosure and its format and content. On the former aspect, disclosures are differently regulated, and accordingly termed ("Suspicious Transaction Reports" -STRs, "Suspicious Activity Reports" - SARs, "Unusual

[15] The two situations may coincide, especially for FIUs that are located within law enforcement agencies where analytical and investigative tasks are strictly linked.

Transaction Reports" - UTRs). Under the second respect, the information content varies to take account of both the analytical needs and the type of reporting entity and of the activities performed.
The vast majority of respondents have indicated that they receive disclosures in the form of STRs. Only few respondents have referred to SARs or UTRs. The differences among these types of disclosures should not be overestimated. In terms of the information content, while STRs focus in principle on specific "transactions" and on the associated anomalies, the scope of SARs is broader as it extends beyond individual transactions and encompasses broader behaviours and operations, considered in their entirety to identify potential links with illegal activities. However, responses clearly show that these differences are to a great extent compensated by the respective information content of STRs and SARs, which is significantly convergent. In fact, while disclosures labelled as STRs generally include information on the overall operational context, SARs, on the other hand, focus also on particular transactions (or subjects).
As regards Unusual Transaction Reports, the difference with respect to STRs and SARs seem to be one of nature and relevance, more than being related to the content. These disclosures, first of all, may be triggered by specifically dedicated indicators set by competent authorities: the reports do not feature outright or full-fledged suspicions and rather stem from the identification of relevant anomaly factors.
The UTR approach may determine difficulties when it comes to international cooperation. In fact, responses show that UTR information may not be available for FIU-to-FIU exchange (at least, not until the disclosure is further examined by the FIU and the case is found to be "suspicious"). Similarly, UTRs may not be considered as "cross-border STRs" and, therefore, neither forwarded to interested FIUs nor made subject to, or utilised in, joint analyses. As regards the relevance and use of UTRs, differently from STRs and SARs, they usually do not trigger the full analytical toolkit of the receiving FIU. This, in fact, only submits these disclosures to preliminary consideration to determine if, in light of subjective and objective elements and other information available, the underlying cases or activities reach the threshold of true "suspicion" or not.

Structure and content of disclosures
Responses clearly demonstrate that the structure and contents of disclosures filed to EU FIUs, in the forms of either STRs, SARs or UTRs, vary to a considerable extent. Differences are not only related to the format but affect the type and extent of the information which is made available to FIUs in different countries as well as the level of details on particular aspects concerning the activities detected, the operational context, the subjects involved, the grounds for suspicion.
What varies significantly in the structure of disclosures across national approaches are: the more detailed articulation which in some cases includes dedicated and extensive references to the characteristics of the suspicious activities detected, the description of the underlying reasons which underpin the suspicion, the overall description of the operational context in which the suspicious activities have taken place and of connections with other subjects or activities.

Implications for analysis and international cooperation
Differences in disclosures are reflected in differences in approaches by FIUs to the analytical functions. The capacity to provide international cooperation and its extent is affected too. As regards the structure and content of disclosures, and the way in which these can shape or influence the analytical function of the receiving FIU, the following considerations can be developed.

- Disclosures based on in-depth scrutiny by the reporting entity and on a broad set of information. Under this approach, the timeframe for filing reports may be relatively longer and the number of disclosures may be lower; "matches" with foreign requests may be less likely but, when they occur, the FIU can provide ample information. Also, a richer set of information allows the FIU to immediately assess the case, limiting the need to request additional information, with the associated delays. The quality of the FIUs' analysis is also expected to be relatively higher.

- Disclosures based on "simplified" examination by the reporting entity, also relying on objective indicators. These are cases where rapidity in the disclosure may be favored over comprehensiveness. The FIU is in a position to receive quick and numerous inputs but may have relatively more difficulties in following these up without resorting to additional information. These cases may lend themselves to a quick dissemination to competent law enforcement agencies, for immediate investigative consideration, rather than to lengthy financial analyses. Matches with foreign requests may be relatively frequent but less information to share may be immediately available to the FIU.

FIUs that perform a law enforcement-type of analysis normally avail themselves of disclosures that are centered around the identification of particular subjects and transactions and their involvement in investigations or connections with investigated subjects. On the other hand, disclosures carrying more articulated information on, e.g., the operational context within which the suspicion has arisen, the economic background of the subjects involved or the associated networks of interest, lend themselves to analyses that are more focused on the underlying economic and financial anomalies.

Like domestic analysis, also international cooperation can be affected by the type and the information content of the disclosures. In principle, more articulated disclosures facilitate the identification of connections with other countries and minimize the need to access external sources to obtain the information requested by a foreign counterpart, to the benefit of timely responses. On the other hand, as detailed disclosures may be less numerous or reported less promptly, the likelihood of identifying matches with incoming foreign requests may be lower than in cases where more disclosures are received, although less rich in content.

The reporting procedure: direct or through third parties

As the FIU's analytical capabilities are, to a large extent, a function of the information received through STRs/SARs, it is important that also in cases of indirect reporting through designated self-regulatory organizations, the information is ultimately forwarded to the FIU promptly and unfiltered.

As already mentioned, it appears that in some cases the disclosures may be made subject to forms of filtering by the self-regulatory body. Filtering information out from STRs/SARs may adversely affect the FIUs' capacity to perform effective analysis on the suspicious activities detected. Even more so, of course, when the filtering goes as far as to allow the self-regulatory body to decide not to forward disclosures to the FIU based on own evaluations.

The reporting procedure: means and channels used

The use of dedicated IT means and procedures assisting the reporting and receiving process is widespread across EU FIUs but some of them have not yet implemented these systems in full or have only done this recently and are still managing the transition from previous arrangements.

Due to the incomplete implementation of IT reporting and receiving tools, in several cases STRs/SARs can still be filed through different channels: paper-based systems continue to be allowed in this context for producing and transmitting disclosures. While responses show that these systems are only used to a limited extent, pending the transition to IT-based solutions, producing, transmitting and processing paper-based disclosures raise concerns about the security and confidentiality of information, as well as about the efficiency of the reporting procedure, possibly affecting the timeliness and effectiveness of analytical activities (and of FIU-to-FIU cooperation).

Cases where FIUs implement external IT packages and tools in support of their own functions, while certainly efficient and advantageous under several important respects, should be considered in light of potential issues deriving from the reliance on support from third parties for functioning, assistance and maintenance, with possible impacts on effectiveness, security and independent operations, also depending on the terms regulating the levels of services

Conclusions on disclosures of suspicious activities

Neither the FIUs' "analysis" function nor the "suspicious transactions" reporting obligation are defined or described in details in the EU AML/CFT framework. This seems to determine a situations where the two influence each other in a feedback "loop" that has to be entirely managed and shaped at the domestic level within each Member State. As a result, the obligations to report and the analytical functions, while closely related nationally and strictly mutually depending in each local system, tend to differ significantly across the EU, resulting in a scenario which is considerably varied and fragmented along national lines.

Differences in the duty to report suspicions by obliged entities and in FIUs' functions are clearly justified and necessary to a certain extent to reflect local circumstances and peculiarities. They can also have an impact on several aspects of the compliance with AML/CFT obligations and of the FIUs' activities and cooperation.

- Differences in STR/SAR/UTR obligations may increase difficulties in compliance by obliged entities that have a cross-border presence or operations and a related need to apply uniform approaches to identify and report suspicions at the firm or group level.
- The STR/SAR/UTR structure and content influence the FIU's capacity to carry out analysis and also the nature of this analysis (geared towards a financial analysis or focused instead on law enforcement-oriented actions), thus exacerbating existing "deviations" from a common approach to "analysis" as an FIU core function.
- Due to different data sets available, the FIUs' capacity to share is uneven and the likelihood of receiving useful information is reduced. Also, faced with the obligation to forward cross-border disclosures, FIUs will exchange reports that are different under several respects (as they reflect national peculiarities) and may not even be "recognized" or usable by the recipient counterparts. The capacity to develop "joint analyses", as also foreseen by the Directive (article 51) may also be affected.

It may be worth considering: a) a more focused exercise on the content of STRs/SARs and on the effects of their differences; b) the setting out of common elements for the disclosure of suspicious activities, through legislation or guidance at the EU level. This could be achieved, for example, by defining a common template for STRs/SARs to be used as a uniform basis throughout the EU. This would also facilitate compliance by obliged entities that have a cross-border dimension, both by allowing to report suspicions uniformly across multiple countries of operations and by improving the flows of information at the firm or group level. FIU-to-FIU cooperation would equally be facilitated as the set of information initially received, and available for the exchange, would be essentially common across Member States.

Other domestic disclosures received by FIUs: **nature and content of threshold-based disclosures**

In addition to mandatory declarations concerning the physical cross-border transportation of cash (Regulation (EC) 1889/2005), responses show that only a minority of EU FIUs receive threshold-based reports. Moreover, the types of the disclosures received by this minority of FIUs are similar to each other, as they seem to converge into few common models. The majority of objective disclosures concern transactions in cash above specified thresholds, consisting in deposits or withdrawals. The threshold that triggers these cash disclosures ranges between 10.000 and 32.000 euro. Other types of objective disclosures are related to fund transfers operations. These are triggered by transactions whose amount is comprised in a range between 1.000 and 30.000 euro.

In few other cases, respondents have referred to further types of disclosures that they receive in accordance with their domestic legal framework, in support of analytical activities.

Declarations on physical cross-border transportations of cash are filed to the national customs agencies. This data, again in accordance with Regulation 1889/2005, is then made available to the FIU either by forwarding the declarations or by providing the FIU with their information content. The forwarding can take place through automatic means. In other cases, Customs provide the FIU

with information on cash declarations through more indirect ways, through ad-hoc communications based on certain features, modalities and timeframes.
In the absence of forms of direct access by the FIU to the database gathering and storing the declarations of cross-border transportations of cash, it is important that the mechanisms in place to forward or share this information with the FIU allow for the necessary rapidity and security. Timely information on activities involving cash (or bearer instruments) may be particularly relevant in terrorist financing-related analyses. While periodic transmission of data packages in structured formats may be efficient but less timely, automatic forms of sharing or transmitting declarations, or their content, may be more conducive to prompt consideration by the FIU (and equally efficient).
For what concerns the other threshold-based disclosures that EU FIUs receive in addition to STRs/SARs and declarations on cross-border transportations of cash, responses show that these are in all cases directly received by the FIUs themselves, in most instances through the same channels and modalities used for the transmission of STRs/SARs.
There are also cases where threshold-based disclosures are transmitted and received through more traditional, paper-based, formats and procedures.
It is important that objective disclosures reach the FIU in a timely manner: firstly, although not reported as suspicious, the underlying transactions may well become such in light of possible additional information available to the FIU, which could therefore need to act quickly upon them; secondly, information in objective disclosures may be directly relevant for ongoing analyses and, therefore, may have to be rapidly considered to better assess the case and determine the most appropriate follow up.

Conclusions on threshold-based disclosures
Threshold-based disclosures are foreseen by the Directive and domestic legislations as tools, additional to suspicious-based reports, aimed at assisting FIUs in their analyses by making information available on activities and transactions which, although not specifically linked to particular anomalies or suspicions, may be relevant for the identification of matches and correspondences with other transactions, as well as for the detection of overall phenomena or trends in particular sectors or through the use of particular tools or operations.
Given that, based on the responses, only a minority of EU FIUs receive threshold-based or objective disclosures (besides the mandatory declarations concerning the cross-border transportation of cash), the question can be asked of whether this tool should be implemented more broadly to expand the scope of the information available to EU FIUs and consequently enhance their analytical capabilities.
While recent experience has indicated that the consideration and analysis of fund transfers operations and remittances are critical for the early detection of terrorist financing activities, only few Member States have introduced measures for the disclosure of transfers of funds as objective transactions. Moreover, these disclosures are in most cases only due for relatively high amounts (e.g. 30.000 euro), whereas terrorist financing may take place through much smaller transactions.
Further reflections may also be needed on whether additional, more varied types of disclosures and information would be beneficial for FIUs to develop effective analysis and reinforce their capacity to identify suspected money laundering and terrorist financing activities.
To address these concerns, the need for more detailed provisions or guidance at the EU level should be considered. Specific types of objective reports could be explicitly set out as mandatory for Member States to implement domestically or, in alternative, as guidance on models to which national practices could converge.
EU provisions or guidance could also be helpful to consolidate types of threshold-based disclosures that, based on the best practices developed by Member States and their FIUs, appear to be particularly useful in support of FIUs' analysis. Based on the results of the survey, as already highlighted, most common types of disclosures which could become models for all Member States are those related to transactions in cash and transfers of funds.

Access to "financial", "administrative" and "law enforcement" information

EU FIUs have confirmed that they have access to financial, administrative and law enforcement information that is required to fulfil their tasks properly. However, the more targeted and granular assessment of responses provided to detailed questions on categories of information available has uncovered several areas of weakness, as well as significant differences across EU FIUs.

These categories of data labelled as "financial", "administrative" and "law enforcement", are not further described in the Directive, thus leaving Member States with a considerable degree of discretion in determining the types of information which may be available to their respective FIUs. This, in turn, translates into significant differences in the range of information available to EU FIUs and, as consequence, in their capacity to carry out effective domestic analysis and develop effective cooperation with foreign counterparts.

General conclusions on FIUs' access to "financial", "administrative" and "law enforcement" information

Responses confirm that EU FIUs have indeed access to considerably diversified sets of information that they variably (and somewhat arbitrarily, in lack of a definition or a common understanding of what these general categories include) label as "financial", "administrative" or "law enforcement". Beneath the issue of definition, lies an issue of scope. In several cases, the range of information available may be too limited to support the FIU's analytical functions adequately. Similarly, differences between, and narrow domestic availability of, information ("financial", "administrative" and "law enforcement") directly impact the FIUs' capacity to provide effective cooperation to foreign counterparts under two complementary aspects.

Some FIUs may have an insufficient range of information available and a correspondingly low capacity to provide assistance in response to requests from foreign counterparts. Moreover, differences in the information available entail discrepancies that can trigger the reciprocity condition and cause refusals to cooperate by those FIUs that, despite having the capacity to provide the requested information, are aware that they would not receive the same information in similar circumstances by the counterpart in question.

To avoid, or limit, these undesired adverse effects on FIUs' activities and cooperation, it may be worth considering to develop a common approach at the EU level on what should be a minimum scope of the information available to FIUs and what types of information should be included, as a common minimum, under the categories of "financial", "administrative" and "law enforcement". In this regard, a higher level of harmonisation seems particularly needed.

Information on bank accounts through centralised databases or retrieval systems

The majority of respondents have indicated that they can have access to information allowing the identification in a timely manner of whether a natural or legal person holds or controls accounts within banks established in their respective territories. However, responses show that this capacity is only in some cases based on the availability of central registers with information on bank accounts or of other centralised systems for retrieving this information.

Such registers or systems are reported to be in place only in some Member States, with their respective FIUs having access to them. Existing arrangements differ considerably across Member States as to the authority in charge of maintaining the central database or system, the nature of such database or system, the information that can be obtained. Some respondents explicitly inform that, particularly for the implementation of the fourth Directive, appropriate regulatory reforms are underway and centralised bank accounts databases are expected to be set up shortly in their jurisdictions.

Based on responses, it appears that information on beneficial owners of bank accounts is not gathered in central registers (where they exist), despite this being an essential element of customer due diligence procedures applied for the opening of banking and financial relationships, with the

relevant data being collected and kept up to date by banks. The possible lack of information on beneficial ownership represents a significant limitation to the completeness and usefulness of centralised bank accounts registers or mechanisms for FIUs' analysis.

Other means of accessing information on bank accounts

Responses seem to suggest that, in lack of centralised means for retrieving information on bank accounts, this information can be obtained by FIUs by approaching individual banks, either directly, based on general information powers available for the analysis (specifically the power to query obliged entities), or through another competent authority such as the sectoral supervisor.

Clearly, the power to obtain information from individual banks is particularly important for the FIU to retrieve data on accounts, their holders and beneficial owners, and the activities performed through them. However, this can only be done in cases where the banks that should be approached are already known. In cases where this objective is pursued by sending requests to all banks established in the territory, concerns arise as regards timeliness, effectiveness and confidentiality.

The capacity to approach individual banks and obtain information on specified accounts, therefore, does not solve the issue of how FIUs, when they do not know where individuals or entities hold their assets, can determine whether these individuals or entities hold accounts in their jurisdictions and, if that is the case, in what banks these accounts are maintained. Only after the questions are responded of "whether" accounts exist and, if yes, "where" they are held, can then the FIU effectively exercise its information powers to approach the identified banks with targeted requests for information on what are the features of the accounts and how they have been used, as needed for its analytical purposes.

Conclusions on FIUs' capacity to determine the existence of bank accounts

Responses received on this point show that only in few cases centralised registers or mechanisms have been set up in EU Member States allowing FIUs to obtain timely information on whether and where natural or legal persons hold accounts in banks established in their territories. While there is not currently an obligation in this respect within the EU, there are strong indications that this is an important tool in support of FIUs' analyses on money laundering and terrorist financing (and, more broadly, for financial investigations in these matters by all competent authorities).

Outside of the few cases where centralised databases or mechanisms are in place, EU FIUs do not seem to have effective capacities to obtain through other means information on whether and where specified bank accounts are held by certain individuals or entities within their jurisdictions. In fact, the exercise of ordinary information powers available in support of the analytical functions vis-à-vis particular banks, as indicated by several respondents that do not have access to central registers or mechanisms, do not seem sufficient for this purpose.

Besides limiting domestic analyses and intelligence, the lack of capacity to obtain this information has also an impact on FIU-to-FIU cooperation. In this respect, while the reciprocity condition might prevent FIUs that can avail themselves of national bank accounts' databases from providing this information to foreign counterparts that cannot, the identification of bank accounts held domestically cannot in most cases be complemented with the identification of accounts held by the same subjects in other Member States.

This information would clearly be particularly important both for domestic analysis and for the development of further cooperation between the interested FIUs on potential illegal activities of a cross-border nature carried out through bank accounts and assets held in multiple countries. The same information would also facilitate consistent, comprehensive and timely application of targeted financial sanctions and related controls.

Information on the identification of assets

Besides "banking registers or electronic data retrieval systems" for locating bank accounts, the vast majority of respondents have indicated that they can have access to information allowing the

identification of other assets. Most common types of accessible information concern real estate. Several respondents inform that they have direct access to centralised land registries, generally by electronic means. However, the types of databases, their contents and the access conditions vary considerably from Country to Country. Some FIUs recall that they can have access to other databases with centralised information on assets held in their countries and their owners. In several cases, registers on vehicles are available; less frequent is the availability of databases with information on shareholdings in companies (although access to companies or business registers, with information on directors and shareholders, may be more common and widespread: see below).

Information on legal and beneficial ownership.

As regards the capacity of EU FIUs to access information on beneficial ownership, responses show that only few of them can obtain such information and that the obligation (for Member States) to set up central registers for this purpose has not been fulfilled yet. On the other hand, companies registers with information on legal entities (including their legal ownership) appear to be widespread and generally available to EU FIUs, although the content of such registers and the information that FIUs can extract from them differ.

Importantly, although only a few, some FIUs cannot obtain information on the legal ownership of companies. They are therefore prevented, based solely on the consultation of companies register, from identifying shareholdings and determine the property structure of legal entities. No reference has been found, in responses, to access specifically to information on trusts or similar legal arrangements.

Other information sources on legal and beneficial ownership

Despite the absence to date of proper central databases with complete information on beneficial ownership, some respondents highlight that they can anyway obtain this information, as needed for their analysis and international cooperation either, through other registers with relevant data or by using other means. A particularly important role seems to be played in these cases by notaries as, in countries that have a notarial system for the setting up of companies and other legal entities and for changes related to their ownership or corporate structure, these professionals are not only required to acquire beneficial ownership information (based on their CDD duties) but are also obliged to provide this information upon request by the FIU and other competent authorities.

Conclusions on access to information on legal and beneficial ownership

The requirement to set up central registers with beneficial ownership information poses significant challenges to Member States. In light of the outcome of the Survey, concerns may arise on the capacity to properly comply with this requirement within the deadline set for implementation (26 June 2017). These concerns are somewhat heightened by findings showing that some FIUs may not have access to company registers in their countries and some of those that do have this access cannot obtain information on the legal ownership of companies.

Several FIUs rely on composite mechanisms that allow them to have access to information on companies, other legal entities or trusts based on different sources and through different procedures. These normally entail consulting separate databases or approaching certain categories of obliged entities (such as companies, professionals, trust and company service providers or financial institutions).

In this regard, it is important to underscore that only a centralised database can allow FIUs to determine if an individual holds beneficial ownership positions, what are the interested entities or legal arrangements and what are the characteristics of the beneficial ownership itself. Other, "decentralised" means, such as the capacity to obtain information from obliged entities (banks, notaries), presupposes that the FIU already knows where the relevant individual or entity holds a business relationships.

Another problem, as also flagged by respondents, is that information gathered by obliged entities may not be complete or duly updated.

Other financial and administrative information

The survey shows that the range of financial and administrative sources of information available to EU FIUs is particularly diverse, also reflecting the FIUs' different natures and objectives. While this range appears to be generally broad, the conditions for the access are variable and in many cases forms of indirect access seem to pose conditions to the FIUs' capacity to obtain information. On the other hand, responses do not refer to existing plans, being considered at the national level, to expand or improve the range of databases or information available to FIUs. Reference is only made to the prospective setting up of central registers of bank accounts and of beneficial owners.

With the exception of these two types of databases, the EU provisions do not foresee particular information sources that Member States have to make available to FIUs for their analyses and international cooperation. The resulting discretion, together with the mentioned differences in FIUs' natures, organizations and analytical functions, appears to be the root cause for the considerable variety and diversity of information sources available to EU FIUs.

Unequal capacities to have access to information may lead, domestically, to less effective analysis, in cases where the scope of available sources is reduced (other conditions being equal). As regards FIU-to-FIU cooperation, FIUs with a narrow range of available databases may be less effective in providing useful information. Cooperation can also be negatively affected by differences in information accessible, due to the lack of reciprocity in cases where the requesting FIU does not dispose of the information sought from the requested counterparts.

Against the background of existing differences, good practices could be identified and shared among Member States and FIUs, thus assisting in identifying information needs in support of quality analysis and cooperation and ways to satisfy those needs. More detailed provisions or indications at the EU level on types of information which qualify as "financial" or "administrative" (in addition to that related to bank accounts and beneficial owners) would certainly facilitate this process of better alignment and improvement of the range of domestic databases available to FIUs. For this purpose, further work needs to be done on the identification of types of financial and administrative information that EU FIUs have access to.

Such a common framework of reference would assist EU Countries and FIUs in the implementation of international and EU provisions and would help reducing discrepancies among EU FIUs that affect particularly FIU-to-FIU cooperation.

Law enforcement information

Faced with an equally general and undefined notion in the Directive, Member States have identified considerably different sets of "law enforcement" information available to their FIUs. Due particularly to the need, in many cases, to access sensitive information held by agencies in charge of criminal investigations or prosecutions, these differences are in several cases rooted into the difficulty for non-police-type FIUs to have access to police databases. This access, although only in few cases and under particular circumstances, turns out to be entirely absent.

Moreover, both the types of data which can be obtained and the conditions and procedures for acquiring them are considerably different across Member States, with significant impacts on domestic activities and on FIU-to-FIU cooperation.

Types of law enforcement information and access procedures

The range and types of police information available vary greatly, particularly as a function of the nature of the FIU and of the relations it has with law enforcement agencies that hold this information. Police-type FIUs have the broadest access, often encompassing all police databases available domestically, under the same capacity accorded to national police bodies. Hybrid FIUs rely normally on requests filed to competent law enforcement agencies or on information channeled

by "liaison officers". Types of accessible law enforcement information include criminal judicial decisions, criminal investigations or prosecutions, criminal intelligence.
Responses show that also the procedures that FIUs have to follow to access these databases vary considerably. Modalities mostly differ depending on the nature of the FIU, its institutional setting and the relationships with police agencies: direct access is a prerogative of FIUs that have a law enforcement nature or have dedicated means of liaising and communicating with competent police bodies; indirect access can be carried out through liaison officers or by means of ad-hoc requests, filed by the FIU on a case-by-case basis. Of course, to different modalities correspond different timeframes for obtaining the information.
Direct access. Police FIUs, set up themselves as specialized law enforcement bodies or otherwise located into national police agencies, have generally ample and direct access to any law enforcement database. Some hybrid or administrative FIUs can also use direct electronic means of communication to obtain information from accessible police databases.
Indirect access. Indirect access can take place through liaison officers (normally police officers who have access to police databases) that extract law enforcement information from relevant databases and provide it to the FIU on a "need-to-know" basis. Other, more traditional modalities of indirect access are based on the filing of written requests by the FIU to the competent police agencies.

Conclusions on the FIUs' access to law enforcement information
In the absence, in the Directive, of a definition of "law enforcement" information, the survey has highlighted the existence of a considerable variety across Member States of police databases available to FIUs. It has also shown cases of difficulty for EU FIUs to have access to a sufficiently broad range of law enforcement information.
There is a considerable "gap" between police or judicial FIUs, that can access a wide array of police databases, and administrative and hybrid FIUs, with a more limited access. Most relevant limitations seem to lie in the availability by the latter FIUs of information related to ongoing investigations or prosecutions, as well as on intelligence gathered outside of legal proceedings or formal criminal investigations.
Existing limitations may impact on the FIUs' capacity to perform effective analysis at the domestic level and to provide a sufficiently broad cooperation to foreign counterparts. In this last respect, possible negative implications triggered by the reciprocity condition cannot be underestimated.
The conditions and procedures for allowing the FIUs' access to law enforcement information also vary considerably, with forms of indirect access which may entail difficulties to obtain timely information.
Remaining cases where FIUs do not have access to law enforcement databases or information should be urgently addressed and solved through appropriate action by the interested Member States.
Indications crafted at the EU level on what types of law enforcement information should be available to FIUs as a minimum would be particularly helpful to foster uniform implementation, approach national solutions and mitigate the undesired effects highlighted above. For this purpose, further work may be considered to more precisely and completely map out police sources that are currently available to EU FIUs and to identify practices which could be shared and implemented across Member States.

4. FIUs' power to obtain information from obliged entities

FIUs should be able to obtain information from obliged entities both for domestic analysis and to respond to requests from foreign FIUs. It is important to note that the power to obtain information from obliged entities should be available to FIUs throughout the entire analytical cycle, until

dissemination: either at the inception, when there is a need to determine whether a case is indeed "suspicious" and qualifies for further scrutiny, or more towards the end, when it is important to complete the analysis and gather information capable of properly steering any possible further action after dissemination.
As regards the scope, FIUs should be able to obtain information from any of the subjects that, based on the Directive and on national implementing provisions, are bound by AML/CFT obligations and regardless of whether or not this same or any other entity has filed an STR/SAR on the case to which the request may refer.

EU FIUs' capacity to obtain information from obliged entities
Responses to the Survey show that EU FIUs still face significant constraints in the exercise of their powers to obtain additional information from obliged entities. These constraints derive from lack of capacity or, in most cases, from the existence of multiple conditionalities related to general domestic laws or procedures, for example on data protection.
FIUs may also lack the capacity to obtain information from obliged entities or be subject to particular conditions or restrictions in cases where investigations or legal proceedings are underway involving the same or related activities or subjects.
Several FIUs do not act upon a dedicated legal basis specifically empowering them to obtain information from obliged entities. Rather, this power is deducted, also implicitly, from general provisions in the law assigning to the FIU an overall power to access external sources or to query third parties.
Responses to the Survey also hint to conditions to the FIUs' capacity to obtain information consisting in the existence of a "suspicion". This condition seems to contrast with the requirement that FIUs should be able to obtain information from obliged entities at any stage of their analysis, even when the suspicious nature of the case under scrutiny has yet to be confirmed or validated and even in order to dispel any potential relevance so that the case can be closed. The condition of the identification of a "suspicion" in order to obtain information from obliged entities can also pose undue limitations to the exercise of this power in the context of FIU-to-FIU cooperation if the requested FIU has to verify or assess, based on its own judgement, the suspicious nature or relevance of the case to which the request refers.

Existing conditionalities (existence of prior STRs/SARs; need for court orders)
The most relevant and widespread conditionality, based on the responses to the Survey, is the existence of prior disclosures on the same case for whose analysis additional information should be sought from obliged entities. Several FIUs can only approach obliged entities with requests for information if prior STRs/SARs have been received on the same case. The condition of prior STRs/SARs being received on the same case seems to play a significant role in narrowing down the scope of EU FIUs' capacity to obtain information from obliged entities.
Some respondents point out that the condition of a prior report but can also be fulfilled when the case is brought to the attention of the FIU through other means, typically through requests or exchanges with foreign counterparts.
In some cases, the FIU can only approach reporting entities to obtain follow-up information on prior disclosures that are unclear or incomplete. More than a power in support of the FIU's analysis, these types of requests seem rather intended to complement the general reporting obligation by allowing the FIU to fill in missing parts of previous disclosures.
Moreover, cases are reported by respondents where the FIU is not able to request information to obliged entities without having obtained a court order to that effect that makes the request enforceable.
The lack of empowerment of the FIU in these cases, and the "substitution" of its decision with an order by a court seems to underlie an assumption that obtaining information which is hold by obliged entities is a measure that falls into the domain of law enforcement and, as such, requires

duly consideration and decision by competent judicial authorities. On the contrary, the provision in article 32(3) of the Directive requires Member States to assign this information power to their FIUs as an administrative tool (which should not raise any law enforcement implication) specifically in support of their analyses.

Conclusions

Responses to the Survey show that EU FIUs generally still lack an adequate capacity to obtain information from obliged entities. Moreover, when they dispose of this power, its exercise may be subject to significant conditionalities that reduce its scope. While the transposition of this (relatively) new power into national laws may still be ongoing, the following points should nonetheless be highlighted. These shortcomings may have an impact on the capacity to carry out effective analysis and provide cooperation to foreign counterparts.

In some cases the FIUs' capacity to obtain information from obliged entities is not reflected in national laws explicitly providing for and regulating this power. The lack of a dedicated legal basis empowering FIUs to obtain information from obliged entities can raise doubts on the existence and extent of the FIUs' capacity to receive information needed for the analysis and for FIU-to-FIU cooperation, as well as potential conflicts with other general domestic laws, restrictions or requirements (such as those on data protection or on financial or professional secrecy).

Conditions limiting the EU FIUs' capacity to obtain information from obliged entities should be removed. FIUs should be allowed to seek information from obliged entities whenever this is needed to perform proper analysis and FIU-to-FIU cooperation. This power should be available for FIUs to exercise generally in the course of their functions, without undue limitations consisting, for example, in the existence of prior disclosures on the same cases or subjects. It should also be clear that this power can be exercised at any stage of the FIU's analysis, that is either at its initial phase (when a full-fledged suspicion may have not yet been formed) or at its conclusion, in order to provide appropriate inputs through dissemination. FIUs should be able to exercise this power directly, without a need for a court order or other authorizing mechanisms. In fact, this is specifically linked to the performance of analytical functions and cannot be considered a law enforcement tool and made subject to authorizations from competent prosecutors or in constraints deriving from ongoing investigations or legal proceedings.

The appropriate empowerment of the FIU is certainly an issue of national implementation. Common EU rules on this matter would be particularly beneficial to provide for a common framework clarifying that FIUs should be able to obtain information from obliged entities whatever this is necessary to support their functions.

5. Domestic functions

The analysis function. Operational analysis

The lack of provisions describing the analysis function entails a great differentiation of its concrete development by the FIUs and make this function subject to influences from the nature, location and role of the FIU within its national AML/CFT framework. While operational analysis is a common feature for all EU FIUs, its character and objectives, therefore, vary considerably across Member States. The structure, tasks and status of the FIU has a significant impact on the sources of information available for analysis, its purpose and the possibility to exchange information with foreign counterparts. Diverging understandings on what "analysis" is and different approaches to what it entails and how it should be carried out may be at the basis of significant "mismatching" in expectations by FIUs when it comes to providing and receiving cooperation.

Distinction between analysis and law enforcement activities

FIUs' analytical functions are distinct from law enforcement and prosecutorial activities conducted on the same phenomena. The former are, in fact, specialised, separated out and assigned to FIUs as competent authorities, in turn different from investigative agencies (even when they have a police status).

Responses indicate that for the majority of law enforcement FIUs the analysis tasks are kept separate, legally and procedurally, from investigative or judicial activities, carried out by the FIU or by the host organisation on the same facts. In two cases, however, respondents have highlighted that a clear demarcation does not exist and that, therefore, analytical and law enforcement activities overlap and are conducted in conjunction. In fact, the relations between analysis and investigation may become somewhat more difficult to discern, or blurred, in cases where the FIU has itself a police status. The closed proximity between the analysis and the investigative stage, or their assignment to the same agency, may make it difficult to draw a precise distinction between these different functions, as the two may be unified in a seamless "continuum". The dissemination itself may become difficult to identify and single out as an autonomous function, as the STR and analysis information may be simply shared or accessed (rather than proactively forwarded by the FIU) within the same organisation.

The absence of a clear distinction between analysis and investigation may affect the FIUs' capacity to perform analysis as an autonomous function, depriving investigations and prosecutions of the added value that, in the logic of the Directive and of international standards, the prior analysis is supposed to bring for the ascertainment of economic and financial crimes.

Moreover, bringing forward analysis and investigation as conjoint activities may impact on the FIUs' capacity to exercise autonomous powers to obtain information from external sources (including from obliged entities) outside of a criminal investigation context and without the conditions and limitations applicable in such contexts.

The scope of operational analysis and the capacity of FIUs to focus on relevant cases

The analysis may focus either on each single disclosure received or on appropriately selected information. The majority of EU FIUs analyze each individual STR, whereas a significant minority conducts operational analysis in selected relevant cases.

The high (and increasing) number of received STRs/SARs has been identified as a challenge by several EU FIUs. To be able to carry out their functions properly, over half of the respondents have implemented a pre-analysis phase, aimed at prioritising the cases or selecting those that require in depth operational analysis. Many FIUs have a selective approach to cases submitted to operational analysis.

The type and volume of the disclosures received, the type of obliged entity and the expected use of the information after dissemination are all elements that influence the thoroughness of the analysis conducted. Conducting an in-depth analysis on every disclosure when the volume of reports exceeds the possibilities of the FIU to process them is not only inefficient, but also can lead to crucial information not being disseminated to competent authorities in a timely manner. The implementation of efficient IT tools and procedures should play a crucial role in supporting the FIUs' analysis and facilitating the selection of relevant cases and information that should be timely disseminated to competent authorities.

Results of operational analysis. Intelligence products suitable for use in investigations

FIUs have indicated that the analysis they carry out specifically aims to develop intelligence products suitable for use in investigations. EU FIUs forward to their competent authorities a variety of different intelligence products. Differences affecting the way FIUs conduct operational analysis, particularly as regards the range and type of information available, have an impact on the quality and usefulness of the final product provided to competent authorities. For example, inadequate access to law enforcement information, especially concerning ongoing investigations and

prosecutions, can result in difficulties for the FIUs to identify existing investigation needs or even become aware of ongoing investigations, thus limiting their capacity to properly shape and address the dissemination action.
It is also important to underscore the crucial relevance of feedback from competent authorities to the FIU on the use of the disseminated information and on the outcome of the investigations performed on the basis of that information, as required under article 32(6) of the Directive.

Strategic Analysis
In line with international standards and EU provisions, responses highlight that strategic analysis assist FIUs in identifying areas which deserve particular attention, so that the analytical efforts and available resources can be properly and efficiently deployed. There is a great variety of products originated through strategic analysis. Money laundering and terrorist financing patterns and trends are examined and in some instances the results are shared with relevant stakeholders through periodic reports. Some FIUs take part in wider analyses conducted by the organization in which they are embedded or conduct trend analysis for other agencies. Many units contribute, through strategic analysis, to the national risk assessment.
The information provided by respondents indicates that FIUs significantly differ in the way they conduct strategic analysis. Differences are visible especially regarding the information sources available and the use of the outcomes.
Money laundering and terrorist financing trends and patterns have frequently a cross-border dimension and strategic analysis should not be merely restricted to the identification of trends and patterns in a particular country, as it seems to be done so far by most of the EU FIUs. It is worth noting that the Directive has introduced the concept of a supranational approach to the assessment of risks with a cross-border nature. Also for these reasons, consideration needs to be given to enhance cooperation among EU FIUs in the field of strategic analysis in order to assess ML/TF trends and patterns more comprehensively.

Spontaneous dissemination. Capacity to select the cases to disseminate
Cases where all the information received is in turn disseminated does not seem to be in line with the provisions of the Directive. In fact, FIUs should have the capacity to perform the dissemination function by ensuring that the cases and the information disseminated are selected in a manner that allows recipient agencies to properly focus their action and use their resources efficiently. While all information received or otherwise available to FIUs have to be considered, relevant cases potentially indicative of money laundering or terrorist financing offences, should be identified. When it comes to dissemination, FIUs should forward to competent authorities relevant information which, in turn, allows law enforcement agencies to focus on priority and develop targeted and effective action. The vast majority of EU FIUs have responded that they select the cases and the information to disseminate, so as to support law enforcement authorities and assist them focusing on relevant cases.

Recipient authorities
The scope of "competent authorities" designated as recipients of the FIU's dissemination varies among different Member States. In some instances it includes also judicial authorities, supervisors and fiscal authorities, besides law enforcement agencies. In several cases FIUs take determinations on which competent authorities should be the recipient of each particular dissemination.
On this point, a more targeted overview may provide helpful insights on existing practices, which could be shared to foster convergence, and a more in-depth understanding of EU FIUs' dissemination systems. This may also facilitate international cooperation, particularly as regards the provision of the consent to forward the information shared to other domestic agencies (as these agencies would generally be known in advance to the requested FIU).

Capacity to provide information on request from competent authorities (dissemination on request)

Several respondents have pointed out that they face no particular legal constraints with regard to dissemination of information to other authorities. Only one FIU indicated that it does not have the capacity to provide STR/SAR information upon request of domestic competent authorities. Several differences have been reported as regards the "competent authorities" to which the FIU can forward STR/SAR information:

The discretional nature of the FIUs' dissemination on request confirms and support the status of autonomy and operational independence of FIUs: these cannot be forced to disseminate information beyond what follows naturally from the outcome of their analysis as a core function in support to ensuing investigations.

Postponement of suspicious transactions

While the majority of EU FIUs have confirmed that they have the capacity to postpone suspicious transactions, others have flagged that they still lack this power which is expected to be introduced following the implementation of the fourth Directive. The lack of powers to postpone a transaction (besides contrasting with the provisions in the Directive) can jeopardize the capacity to promptly restrain criminal funds or assets, also for seizure purposes.

The duration of the FIUs' postponement varies greatly across EU FIUs. It ranges from two days till an unlimited time. Taking into account the cross-border nature that criminal financial activities frequently assume, and the need to ensure that suspicious transactions can be postponed effectively also in the context of FIU-to-FIU cooperation, diverging durations of the postponement can have detrimental effects on FIUs' action and cooperation. More uniform approaches would benefit the overall capacity to stop and seize criminal funds in cross-border situations. The need for more uniformity in the postponement function should be emphasized also in light of the new obligation for FIUs to forward cross-border reports to interested counterparts and of the duty to postpone suspicious transactions also on behalf of foreign counterparts.

Differences among national systems exist also in the applicable procedures (whereby some may be exposed to risks of tipping-off and lack of confidentiality) and in the subjects involved. More detailed provisions at the EU level would seem necessary to tackle these issues by ensuring more uniform and convergent approaches by FIUs, which would in turn foster effectiveness and facilitate cooperation.

Conclusions

Taking into account the increasing volume of disclosures received from reporting entities the capacity of FIUs to be "selective", throughout their analysis up until the dissemination of its outcome becomes crucial both to ensure an adequate treatment to disclosures according to priorities and to allow law enforcement agencies to focus on substantiated money laundering or terrorist financing cases.

Provisions or guidance at the EU level on the nature and features of "analysis" as a core and independent FIUs' function may bring considerable benefits.

Respondents have underlined problems in coping with constantly increasing volumes of disclosures received. In some instances, these problems are aggravated by the lack of appropriate IT systems to assist them in performing this function. Member States and FIUs should be encouraged to develop IT resources in support of analytical functions.

Postponement regimes feature several different approaches; for example, the duration of the suspension varies considerably across Member States, with potential difficulties for the postponement of activities that have a cross-border nature through FIU-to-FIU cooperation.

6. Cooperation with other FIUs

Capacity to exchange information

The distinction between analysis and investigation is not always neatly drawn and these two tasks may not be separated in a sufficiently clear-cut manner in all cases, both as regards domestic FIUs' functions. Cases where the analysis tends to be merged or absorbed into law enforcement activities bring consequences on the FIUs' ability to engage properly in FIU-to-FIU cooperation.

This happens, for example, because FIUs could have a limited capacity to exercise independent powers to gather information needed to foreign counterparts, either because it is prevented from doing this due to ongoing investigations or because it is subject to an authorisation by a competent law enforcement agency or prosecutor. Equally, FIUs may be prevented from providing information to foreign counterparts because, for example, this information can only be shared through police or judicial cooperation channels.

It is important to stress the need to maintain analytical activities and law enforcement tasks separate. Appropriate action at the EU level should be considered to, first of all reinforce and clarify the distinction between analysis and investigation, both as regards FIUs' domestic activities and their cooperation. The "purpose limitation"[16] should equally be confirmed and detailed in its implications, clarifying that information should be exchanged by FIUs regardless of law enforcement concerns and that the information exchanged is to be used by the receiving FIU exclusively for analysis.

Police and judicial FIUs: separation between FIU's cooperation and law enforcement or judicial cooperation

FIUs that have a police or judicial nature and that may be in charge of both analysis and investigation functions need to keep the two separate. On this point, while respondents generally confirm that this separation is ensured in most cases, the Survey highlights areas of potential problems.

The lack of a clear demarcation between analysis and investigation reflects on the EU FIUs' capacity to have access to information, as this can be limited by the absence of a recognised area of autonomous analytical function for the FIUs. As a consequence, these may be inhibited or made subject to conditions in accessing information when investigations or legal proceedings are ongoing or when the information needed is considered to be accessible only through law enforcement measures or powers. Moreover, there are cases where EU FIUs' analytical functions are not kept separate from law enforcement activities and this impacts on the effectiveness of these functions in bringing added value to ensuing investigations as well as on the dissemination function, as STR/SAR information, rather than being forwarded after analysis, can be used upfront for both analysis and investigations.

Capacity to use domestic powers to obtain and provide information to foreign counterparts

The obligation to use domestic powers to respond to foreign requests needs to be better rooted in national legislations, particularly through an explicit and dedicated legal basis which unequivocally empowers the FIU to use its powers on behalf of other FIUs. At the same time, details should be provided on the extent and scope of this duty, to avoid both uncertainties in national implementation and different approaches being taken by requested FIUs. Provisions or guidance in this regard should be set out at the EU level.

For example, clarifications would be helpful on the need to exercise domestic powers with a view to providing the most appropriate assistance possible in light of the case and commensurate to the information needs of the requesting FIU. Also, available powers should be used, and information

[16] That is the confinement of the FIUs' mandate to the analysis (as opposed to investigation) of suspicions (different from already identifiable criminal behaviors) of money laundering and terrorist financing cases.

sources accessed, taking account of concurrent elements such as the specific demands formulated by the foreign counterpart, the features of the case underlying the request, possible elements on the case which are available domestically (as a consequence, for example, of ongoing analyses or investigations or the involvement of particular subjects).
While underscoring the importance of well-motivated requests, insufficient motivation cannot be per se a valid ground for declining requests for cooperation and, more specifically, to refuse to exercise domestic powers to obtain information. In such cases, counterparts should enter into a dialogue to clarify the context of the request, the information needs and target the exchange accordingly.

The condition of reciprocity
Based on an assumption that provisions applicable to EU FIUs and to their cooperation are particularly homogeneous, the fourth Directive does not explicitly mention the condition of reciprocity as a prerequisite for EU FIUs' cooperation. As a consequence, it seems that EU FIUs should not refuse or limit cooperation with other EU counterparts on grounds of lack of reciprocity.
While the fourth Directive allows for refusing to exchange information when this contrasts with "fundamental principles" of national law (article 53(3)), it is not clear whether this scope includes the condition of reciprocity (which does not seem to qualify per se as a "fundamental principle"). Refusals to provide cooperation on the grounds of possible lack of reciprocity do not seem admissible as they would contrast with the general obligation to provide cooperation in accordance with article 53(1). Clarifications on this point through EU provisions would certainly be helpful.
However, responses to the survey indicate that, based on domestic laws, the majority of EU FIUs are bound by the condition of reciprocity. Reciprocity can play adverse effects on international cooperation, both as regards its extent and its effectiveness. These effects can be amplified by the enlargement of FIUs' powers and capacity to access information, as brought about by the Directive, and by the continued existence of differences and discrepancies among national frameworks.
In all areas where differences exist reciprocity can be lacking, despite the common (but not sufficiently uniform) EU legal framework. Each such area can host a number of potential triggers for the reciprocity condition, thus obstructing FIUs' cooperation. The combined effect that discrepancies and reciprocity can have on the capacity of EU FIUs to provide adequate cooperation cannot be underestimated.
Areas where the lack of the reciprocity condition seems more likely to arise and its effects appear more prominent include the following: different types of information; capacity to exercise domestic powers to obtain information on behalf of counterpart FIUs; capacity to share information with other FIUs; capacity to provide the consent for further use or dissemination of the information exchanged; capacity to provide cooperation to foreign counterparts that are not FIUs; capacity to share information on cross-border STRs/SARs; capacity to engage in joint analyses; confidentiality and data protection conditions.
It is important to confirm explicitly that the reciprocity condition cannot be applied by EU FIUs in their reciprocal cooperation. At the same time, work needs to be done at the EU level in support of the assumptions which lie at the basis of the need to provide cooperation regardless of reciprocity considerations, notably that applicable national regimes are properly harmonized and EU FIUs have equivalent capacity to cooperate. In fact, a prohibition to refuse cooperation on reciprocity grounds remains "credible" and sustainable only if EU FIUs' become capable, to exchange information and provide cooperation based on equal conditions and on a comparable extent and quality level, thus being able to "reciprocate" any response.

Need for a clearance or authorization from a third party
The FIUs' capacity to freely exchange information appears unduly limited by cases where the exchange is subject to authorizations or clearance that must be obtained from domestic third parties. This happens especially when investigations or legal proceedings are underway in the country of

the requested FIU or where the requested information has to be obtained from another agency. Similar limitations to FIUs' cooperation apply in relation to the release of the prior consent for further use or dissemination of the information exchanged. These restrictions seem to depend mostly on the following factors:

- an excessively narrow implementation of the principle of "free exchange of information for analytical purposes" among FIUs (article 53(3) of the Directive, which certainly forbids refusals related to the mere existence of investigations or legal proceedings) and of the duty to provide the prior consent "to the largest extent possible" (article 55(2));
- an excessively broad transposition of the derogations clauses for the exchange and for the prior consent, respectively in article 53(3) (which refers to "exceptional circumstances where the exchange could be contrary to fundamental principles of national law") and in article 55(2).

A more adequate and uniform implementation of these fundamental provisions across EU Member States could be encouraged and facilitated through guidance issued at the EU level, based on legislation or other suitable means, clarifying that the duties to provide cooperation, either through the initial exchange or through the consent for further use or dissemination of the information exchanged, cannot be limited by prior domestic authorizations.

Cases where the exchange of information can be refused

The capacity to provide cooperation through the exchange of information is a fundamental and essentially unconditioned function for FIUs under the fourth Directive. It seems to be well established across Member States. Nonetheless, there are significant exceptions that appear to exceed the scope of the derogations allowed by the EU legislation (and by international standards as well). The Directive allows for refusals to the exchange only under very limited circumstances. These can only be rooted in "fundamental principles" of national law which may be exposed to violation; in addition, the exceptions should be specified ex ante (in national law or regulation), in a way which prevents misuse and does not unduly limit the general rule of "free exchange of information for analytical purposes".

Existence of investigations or legal proceedings

It appears that, either because of the need to obtain ad-hoc authorizations on a case-by-case basis or due to outright prohibitions to exchange, FIU-to-FIU cooperation is still significantly affected by the existence, in the country of the requested FIU, of investigations or legal proceedings, in contrast with the rule of "free exchange of information for analytical purposes". These constraints and limitations may become even more significant, after the initial phase of the exchange, when it comes to providing the consent for further use or dissemination of the information transmitted.

A better implementation by Member States of EU rules on these aspects is certainly needed. At the same time, existing EU rules could be clarified and strengthened, particularly by narrowing down the scope for derogations to the FIUs' duties to cooperate, even in presence of investigations or legal proceedings.

Identification and type of predicate offences

Other significant constraints and limitations to the FIUs' capacity to exchange information derive from requirements concerning the indication in the request of the underlying predicate offence of money laundering and of the type of this offence.

Although responses seem to indicate that only few FIUs have a necessity to receive, in the requests filed by foreign counterparts, an explicit reference to a predicate offence and a description of such offence, some respondents highlight that the exchange of information can indeed be refused when the crime related to the case for which cooperation is sought is not criminalised. Some FIUs in this group have also clarified that, in order to be able to provide information, the request should outline

a case of potential money laundering (or terrorist financing), a link with a suspected predicate crime and its nature, so that the proportionality of the requested assistance can be evaluated.
Responses indicate that cases where cooperation is refused because of differences in the criminalisation of predicate offences often concerns tax matters.
FIUs' cooperation, carried out to support the analytical function, should not be conditioned by the consideration of possible predicate offences. Neither the existence of a particular offence nor its type or nature should become an element of consideration for the requested FIU to provide cooperation.
While Member States should ensure an appropriate implementation of existing provisions in the fourth Directive which prevents FIUs from refusing cooperation due to considerations on the underlying offences, these EU provisions should be clarified and strengthened to better reflect the general rule of cooperation and free exchange of information among EU FIUs. These provisions should more clearly state that FIUs' cooperation, particularly at the stage of the initial exchange for internal analytical purposes, should not be conditioned to the indication of particular offences or to the type of such offences.

Motivated requests
Responses to the Survey show that for several FIUs the adequate description of the case represents an essential prerequisite for being able to share information: this can only be provided when the case under analysis is adequately described in the request and the underlying money laundering or terrorist financing suspicions are properly indicated. In any event, while the majority of EU FIUs require motivated requests as a condition to respond, only some of them would simply refuse cooperation when this condition is not fulfilled.
It is indeed important that FIUs, when requested for cooperation and provided with appropriate motivation, do not refuse to share the information because they assess the case, and the inherent suspicion, differently. Second-guessing the suspicious nature of a case and refusing cooperation on this ground would go against FIUs' obligations to cooperate.
The fourth Directive, while setting out the two "twin" obligations to provide cooperation (for the requested FIU) and to file properly motivated requests (for the requesting FIU), does not make it explicitly clear what is the relation between the two and, more particularly, whether the duty to cooperate may not apply in relation to requests that are not adequately motivated.
To avoid undesired effects on FIUs' cooperation, or uneven applications of these provisions by different FIUs or Member States, the following clarifications, if reflected in EU provisions or guidance, would be particularly beneficial in support of appropriate national implementation and uniform FIUs' practices.

- The rationale behind the obligation to file motivated requests is not to allow the requested FIUs to assess the case by second-guessing it and decide whether and to what extent cooperation should be granted; it is rather about allowing the requested FIU to understand the case and the information needs in order to provide the counterpart with appropriate cooperation.
- In fact, the general obligation to provide cooperation in support of the analysis of potential money laundering or terrorist financing cases, as stated in article (53(1), has an absolute nature and cannot be derogated for the simple reason that requests do not bring adequate information.
- In case of poorly motivated requests, therefore, the cooperation should not be refused. While the requested FIU should provide any possible initial feedback (e.g. based on available STR/SAR information), the involved FIUs should enter into a dialogue to clarify the case and the information needs.

Completeness of the information shared - Financial and administrative information

The survey highlights that, although many FIUs can share financial and administrative information, there are significant cases where considerable impediments and conditions continue to exist to the completeness of responses. These pertain to prohibitions to forward particular types of information (especially that obtained from other domestic entities) and also to outright lack of capacity due to the need to pursue separate law enforcement cooperation channels. These are circumstances where the requirements to exchange information, stipulated in the Directive, do not seem to be complied with.

While national implementation of existing EU provisions should be improved by enlarging and enhancing FIUs' access and capacity to exchange financial and administrative information, more detailed minimum standards in this regard should be set out at the EU level.

Another point to reinforce is that the exchange of financial information should always be possible through the FIU-to-FIU channels and that refusals based on the need to use the Mutual Legal Assistance designed for law enforcement or judicial cooperation should not be admitted.

Law enforcement information

The requirements under the Directive envisaging that FIUs should freely dispose of and exchange, i.a., law enforcement information does not seem to be fully or properly implemented in all cases. Two concurrent factors seem to lie at the basis of existing problems for EU FIUs to exchange law enforcement information.

On the one hand, EU FIUs encounter significant limitations and difficulties in accessing law enforcement information at the domestic level, particularly because the range of available or accessible law enforcement information is often particularly narrow and the procedure to access this information is often indirect and entails approaching or liaising with third parties with limited possibilities for direct enquiries.

On the other hand, law enforcement information available to FIUs, besides being often partial or incomplete, is also frequently subject to conditions in its exchange with foreign counterparts; the FIU may need a prior authorisation for this purpose from the domestic law enforcement body owning and providing the information.

While Member States should ensure a better implementation of the EU provisions on this matter by allowing FIUs to access and exchange police information more broadly and swiftly, more details could be provided at the EU level by, for example, specifying the law enforcement information that, as a minimum, FIUs should be able to access and share and explicitly prohibiting undue limitations or conditions, particularly in the forms of cumbersome access procedures at the domestic level or needs to obtain authorisations from third parties.

Use of domestic powers to respond to requests from other EU FIUs

Responses to the Survey indicate that the requirement for FIUs to use their domestic powers to obtain and share information with other EU counterparts is widespread across Member States. However, it appears that this requirement is not always reflected in laws or regulations.

More explicit and detailed national provisions empowering and requiring FIUs to use domestic powers also for cooperation purposes may be appropriate to ensure an adequate implementation of the Directive on this point. These provisions should more firmly root this requirement into the FIU's toolkit and range of activities, against any possible doubts as to whether the FIU is enabled and required to exercise available powers for international cooperation purposes. This would also be helpful to address legitimate concerns related to data protection safeguards and as to whether these should prevail over the duties to share information with foreign counterpart.

National provisions may also be appropriate to determine the extent to which domestic powers should be exercised to respond to foreign requests, for example by clarifying that the FIU has certainly a duty to exhaust all available means to provide the information needed but that not all the information powers should be activated in all cases, as they should rather be proportionate and

calibrated in light of the case and in accordance with the information needs specified by the counterparts.
Common and uniform indications in this regard could also be set out at the EU level. This would not only provide guidance and a framework for this important aspect of FIU-to-FIU cooperation but would also limit discrepancies and differences among FIUs capacity to access and share information.
Several respondents have stressed the need, in order to be able to exercise domestic powers for obtaining information, that requests be particularly specific as to the motivation, describing the case and the associated information requirements in sufficient details.

Scope of available powers
As regards the scope of the EU FIUs' capacity to obtain and share information by making use of domestic powers, responses show that these are in some cases subject to conditions. As regards external queries, limitations are mostly related to the types of information (as some can only be transmitted through police channels), to the agencies that have to be approached (as not all can allow their data to be shared with foreign FIUs through the FIU-to-FIU channels), to authorizations that are foreseen by these authorities, to the prohibition to obtain and share tax-related information and, again, to the condition of reciprocity.
In addition to general limitations to the capacity to provide cooperation, specific constraints apply to the exercise of FIUs' powers to obtain information destined to foreign counterparts. In some cases, as mentioned, information from domestic obliged entities can only be obtained when an STR/SAR has already been reported by the relevant obliged entities on the same case. Other restrictions are encountered by FIUs when it comes to obtaining and sharing banking and financial information. The FIUs' capacity to use domestic powers to obtain and share information is also inhibited in several cases when investigations or legal proceedings are underway on the same matters. As also mentioned, some FIUs cannot obtain information and share it with foreign counterparts if the (possible) predicate offence underlying the case to which the request refers is not indicated or, when indicated, it is not criminalised in the same form under domestic law.
Where requests are not adequately substantiated, requested FIUs may not be in a position to obtain information by making use of their domestic powers.
The limitations which, according to the responses, significantly hinder the FIUs' capacity to make use of their powers to obtain information on behalf of foreign counterparts do not seem in conformity with the Directive. While FIUs' seem to rely in several cases on general provisions empowering them to access domestic data sources, dedicated implementing provisions are needed for a proper and unequivocal transposition of these EU provisions, allowing (and requiring) FIUs to exercise these powers also to provide cooperation to foreign FIUs.
At the same time, more specific indications at the EU level would also be helpful to ensure a common understanding and a uniform approach across EU Member States and FIUs on the extent of the duty to provide cooperation and on the need to avoid that this is unduly constrained.
There is a risk that FIUs may exercise considerable discretion in assessing the case and the merits of the suspicion, refusing to use their powers to gather requested information (thus denying cooperation, in all or in part) if they deem the request as not sufficiently substantiated, the suspicion not adequately founded or simply the case not sufficiently "serious" (for example, due to the type of the predicate offence).
There seems to be a delicate balance to be struck between the need for appropriate motivation (and the consequent right for the requested FIU to be fully appraised of all relevant facts) and the assessment of requests for the exercise of domestic powers to gather information.
Clarifications through provisions or guidance at the EU level on these points should be considered.

Cross-border STRs/SARs

The obligation to forward to foreign counterparts STRs/SARs "which concern another Member State" is not dependent on requests filed by other FIUs. Also, differently from the spontaneous sharing, this task is a mandatory feature under article 53 of the Directive. This is therefore an innovative obligation for FIUs, consisting in automatic and compulsory forms of disclosure.

Legal basis for sharing cross-border STRs/SARs

Based on responses to the Survey, it appears that in the vast majority of cases, FIUs' capacity to share "cross-border STRs" does not derive from newly adopted provisions specifically transposing article 53(1) for this part. In fact, many responses specify that domestic implementing provisions are still lacking and that disclosures of information related to cross-border STRs are carried out by means of the general capacity to provide information spontaneously (as foreseen by a different provision in the same article 53(1) of the Directive).

This cannot be considered sufficient to meet the requirement under the Directive on the sharing of cross-border STRs/SARs, particularly because, as said, the sharing of disclosures that concern other Member States is, under the Directive, an outright obligation for FIUs, not a spontaneous and, as such discretional initiative of interested FIU.

Conditions and limitations to the sharing of cross-border STRs/SARs

Several types of filters are currently applied by FIUs to the sharing of cross-border STRs/SARs. The requirement of automatic disclosures of these reports is limited by constraints at national level that prevent FIUs from forwarding information without a prior "validation" through analysis (or investigation) which confirm that the case is properly substantiated. These constraints add on to general conditions and limitations surrounding the EU FIUs' capacity to share information (such as those related to the existence of criminal investigations or legal proceedings or STRs concerning tax matters).

Pending the implementation of the fourth Directive, too firm conclusions cannot be drawn on existing shortcomings affecting the EU FIUs' capacity to share cross-border reports. In any event, it is important to stress that the obligation to forward cross-border STRs/SARs needs to be properly implemented in Member States based on appropriate legal bases. Existing provisions empowering FIUs to share STR information spontaneously with foreign counterparts is not sufficient to satisfy this new requirement.

In accordance with the Directive, these 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.

In the absence of a definition in the Directive of STRs/SARs that "concern another Member State", there is certainly a need to specify the scope of this obligation by setting out appropriate criteria in applicable laws or regulation.

It would be clearly appropriate, and even necessary for the implementation and practical application of this provision, if more detailed indications and criteria to determine when an STR/SAR may qualify as having a "cross-border" nature were defined at the EU level, so that discrepancies can be avoided in the application of this EU-wide obligation. These criteria have to be set having in mind, on the one hand, the need for sharing actionable disclosures. On the other hand, appropriate criteria should result in an exchange regime which is manageable, in light of the potentially massive amount of STRs/SARs that may be considered to qualify as of "interest" for other Member States. Several respondents have flagged this aspect as one of the most relevant in the implementation of the new EU AML/CFT framework, indicating that, depending on how this implementation will be realised, significant feasibility and resource implications may arise for FIUs.

"Known/Unknown" exchanges

The vast majority of respondents have confirmed that they can engage in "Known/Unknown" exchanges and respond to requests lacking motivation which are specifically filed with the intent to obtain feedback on whether particular subjects have been reported in STRs/SARs (or are otherwise present in the databases of the requested FIU).

It is not clear, though, if the capacity to respond to requests bearing no description or motivation, although limited to a "hit/not hit" feedback is rooted in national laws specifically authorizing the FIU or if this capacity is simply derived implicitly from the absence in these laws of prohibitions to proceed in this respect. An explicit legal basis allowing the FIU to engage in "Known/Unknown" exchanges might be appropriate to overcome possible uncertainties associated with, for example, data protection concerns, as mentioned, or constraints related to "proportionality" which, as seen, in some cases lead FIUs to decide whether, and to what extent, a response should be provided "weighing" the substance and importance of the underlying case (which, of course, in "Known/Unknown" exchanges is not referenced).

Matching of data sets

Another innovative feature of FIUs' cooperation brought about by the fourth Directive is the obligation for EU FIUs to apply "state of the art technologies" allowing "to match their data with that of other FIUs in an anonymous way". This reference (in article 56(2)) is primarily to "matching" tools developed in the context of the FIU.NET. Similarly to the "Known/Unknown" exchanges, the data matching results in "yes or no" responses, depending on whether or not some of the same subjects are present in the data sets shared by the FIUs involved (following secure protocols ensuring that these data sets are anonymized).

Positive "hits" are similar to "known" feedbacks in "Known/Unknown" exchanges but bring more information, as the FIUs involved were not aware in advance of the link with other jurisdictions. These positive results can be followed up by the FIUs involved in the matching exercise through ordinary motivated requests and comprehensive responses, in accordance with general rules.

Several respondents have indicated that they do not have the legal capacity, based on domestic legislation, to share in an anonymous way entire data sets extracted from their own STRs/SARs databases to identify matches with other EU FIUs. Consistently, many FIUs have reported that, as a matter of fact, they do not use the matching tools provided by the FIU.NET system to identify matches in shared data sets.

While in some cases data protection concerns (also in relation to the actual anonymity of the procedure) seem to play an important role in preventing EU FIUs from participating in matching exercises, it is important that this requirement be implemented by setting an appropriate domestic legal basis. Based on developing practices, and on the overall legal framework that will result from national transpositions of the Directive on this point, the need for common guidance or provisions at the EU level might be considered.

Joint analysis

Another innovative element mentioned by the Directive in the framework of FIU-to-FIU cooperation is the reference to "joint analyses", in relation to "cross-border cases" (article 51).

Cases that involve multiple jurisdictions become increasingly frequent and significant, also due to activities performed by obliged entities on a cross-border basis. These may include, for example, those conducted by financial groups operating in different Member States as well as activities carried out abroad under the free provision of services regime.

To limit the risk that, while information is amply shared and integrated at the EU level, particularly for the identification of cases of common interest, analyses on these cases remain separated at the national level.

Legal basis for joint analysis

The majority of EU FIUs have indicated in their responses to the Survey that they can take part in joint analyses, both on a bilateral and on a multilateral basis. However, responses highlight that this capacity is based on general domestic provisions empowering the FIU to entertain cooperation with their foreign counterparts, basically through the ordinary exchange of information. In this respect, the responses seem to assume that the same capacity to share information can adequately support also the participation in joint analyses.

Therefore, while respondents have confirmed that there are no restrictions explicitly preventing EU FIUs from engaging in joint analysis, it appears that there is equally no explicit authorization or empowerment to cooperate in the conduction of analyses beyond the exchange of information.

Conditions and limitations to joint analysis

It is not surprising in the current picture that several conditions and limitations to EU FIUs' capacity to participate in joint analyses are put forward by many respondents. The Survey shows that provisions specifically addressing the performance of joint analyses seem still lacking across EU Member States.

It is not clear if the FIUs' capacity to share information and cases, as broad as this may be or become following the proper implementation of the fourth Directive, can support all the activities which can be associated with joint analysis exercises in the absence of dedicated provisions.

In fact, also based on further details that can be set out by the EU FIUs' Platform in accordance with article 51, joint analysis may entail activities beyond the sharing of cases, such as the formation of joint teams of analysts which, through appropriate access to databases of their respective FIUs, conduct common evaluations. These may in turn lead to shared outputs and, although each FIU should of course proceed to dissemination to competent authorities in accordance with its domestic legal framework, coordination for consistent follow up in interested Member States may also be expected.

Ad-hoc and targeted provisions may be necessary for FIUs to be able to safely take part in these activities, also in light of coordination with domestic tasks and possible data protection concerns.

Appropriate national implementation of course plays an essential role. At the same time, common provisions or guidance at the EU level would greatly facilitate this process and limit the risk of inconsistent approaches. Also, in line with the provisions in article 51, the EU FIUs' Platform, valuing recent experiences gained through pilot projects on joint work for the analysis of specific issues, should provide guidance on what this particular cooperation activity entails, beyond the exchange of information, and outline a common "methodology" that could assist FIUs in future exercises.

A supranational approach to FIUs' cooperation – a "Financial Intelligence Unit of the EU"

Money laundering and terrorist financing suspicious cases dealt with in STRs/SARs and in FIUs' analysis increasingly have a cross-border nature, in at least two connected respects: potentially illicit activities to be analysed are carried out in, or otherwise involve, multiple jurisdictions; the obliged entities that need to be approached to obtain necessary information and follow the money trail are established or operate in different countries.

The FIU-to-FIU cooperation in the EU should go beyond the model of FIUs international cooperation which is essentially based on the exchange of information on a case-by-case basis, accompanied by certain conditions and safeguards, while the analytical functions continue to remain essentially separated and mostly fragmented along national lines.

The fourth Directive addresses these weaknesses to some extent through a two-pronged strategy: require the sharing of "cross-border" reports; foster the conduction of "joint analyses" on cases that are of interest of more than one FIU. These innovative mechanisms are extremely important but are affected by some intrinsic limitations and should be considered as intermediate steps of a process that should lead up to more advanced forms of coordination at the supranational level.

To pursue such supranational approach, a centralized Financial Intelligence Unit of the European Union ("FIU of the EU") could be set up and entrusted with tasks particularly focusing on the identification of cross-border cases, the consideration of such cases to promote cooperation among national FIUs, the setting up of mechanisms and projects for the conduction of joint analyses. More specifically, an FIU of the EU could perform the following functions:

- facilitate the identification of relevant cross-border cases (based on disclosures from national FIUs but also through the "matching" functionalities of the FIU.NET);
- foster and coordinate the exchange of information between the FIUs involved in the identified cases;
- promote and coordinate joint analyses among European FIUs on cross-border cases that have elements of common interest.

Besides coordinating and facilitating national FIUs' analytical and cooperation functions, the FIU of the EU could perform additional tasks in support of FIUs' activities which would benefit from a more uniform approach at the EU level, for example as regards the development of common approaches to the content of domestic disclosures and to available information sources. It could also ensure a more effective dialogue and cooperation with EU supervisory and law enforcement agencies than what is currently possible.

It is important that any arrangement in which FIUs' functions, both as regards cooperation and analysis, are attributed to a newly created centralised EU body, is set up under appropriate conditions of autonomy and independence. These conditions of independence should apply both to national FIUs (as they should continue to act autonomously and independently from each other and with respect to the EU FIU) and to the EU FIU should itself (as it should remain independent from both national FIUs and from other agencies, at national or EU level).

Use of the information exchanged

All respondents have confirmed that, in conformity with the rule of "purpose limitation", they ensure that the information exchanged is used only for the purposes for which it was sought or provided and is not disseminated or further used without the necessary prior consent of the foreign counterpart.

Respondents also emphasize that any authorized dissemination of the information received from other EU FIUs is carried out with all appropriate safeguards to ensure that the subsequent use (normally only possible "for intelligence purposes") strictly adheres to any limitation or condition related to, for example, the purposes and the subjects that can be involved.

However, some respondents note that, when they provide a consent for further use or dissemination of the information transmitted, together with caveats and conditions, they often realize that this information is treated or disseminated beyond the scope of the authorization. FIUs also note that often times they lose the control on the information disseminated and that it is not possible for the disseminating FIU, despite the scrupulous adherence to all conditions set by the foreign counterpart and any best effort deployed, to monitor the use of the information along the domestic "dissemination chain". These difficulties are particularly relevant when the dissemination is done to prosecutors.

Consent for further use or dissemination of the information exchanged

The prior consent is a key element both for effective domestic analysis and for international cooperation: exchanging information to develop good analysis, even to the broadest extent possible, is useless if this information cannot be disseminated, when needed, due to the absence of the required consent. The more the consent is denied, the more FIUs' cooperation is frustrated and becomes ineffective, together with the associated analysis. It is not by chance that, in fact, the Directive makes it an obligation for FIUs to provide the consent for further use or dissemination, when requested by EU counterparts. More precisely, article 55(2) establishes that "Member States

shall ensure that the requested FIU's prior consent to disseminate the information to competent authorities is granted promptly and to the largest extent possible".

Capacity to provide the consent

EU FIUs confirm in their responses to the Survey that they are able to grant the prior consent to further use or dissemination of the information provided promptly and to the largest extent possible, as required by article 55 of the Directive. The EU FIUs' capacity to grant the prior consent, however, seems to encounter considerable limitations due to a range of conditions applicable in several Member States. These limitations and conditions are variably rooted in the overly general derogation clauses referred to in article 55(2) to the duty to provide the consent. Moreover, ample room is left for discretion, as it appears that in many cases FIUs, under national law, are only allowed to provide the consent, rather than required to do so.

Responses also suggest that, in some cases, the scope of exceptions may be broader than the area of cases where the FIU is required, or even simply empowered/allowed, to grant the consent. Given these circumstances, the consent may be the exception rather than the rule.

On the other hand, the considerable room left to national implementation also translates into significant differences among EU FIUs as to the cases and conditions under which the prior consent can be granted or refused. These discrepancies not only add on to the difficulties of FIUs' cooperation stemming from the need to take account of different regimes for the consent applicable to FIUs engaged in exchanges; they also play an indirect, but more general, adverse role on cooperation via the reciprocity principle.

The requested use or dissemination "falls beyond the scope of application of domestic AML/CFT provisions"

The vast majority of EU FIUs have confirmed that they are bound by limitations in granting the consent when this goes beyond national AML/CFT provisions (based on a case-by-case evaluation). The majority of EU FIUs are prevented from providing their prior consent, or are subject to particular conditions or limitations, due to the type and nature of the alleged underlying offences, specifically depending on whether or not they are also criminalized in their domestic legislation.

Indication about the possible underlying criminality may not be available to the requesting FIU. This, in fact, may only possess the intelligence deriving from the analysis developed that far. The threshold consisting in the description of such crimes can therefore prove inappropriate and excessively high to allow for meaningful FIU-to-FIU cooperation in the dissemination phase. For these reasons, cooperation may encounter significant limitations in these instances.

It has to be added that "dual criminality" conditions are not specifically envisaged by the Directive at the FIUs' level of cooperation. The Directive does not deal, in fact, with law enforcement or criminal law matters, where the "dual criminality" requirement typically lies. This constraint, in fact, is indeed applicable to police and judicial cooperation mechanisms, which are geared toward the identification of evidence to be used in legal proceedings for purposes of, i.a., criminal conviction, seizure or confiscation. It would not seem appropriate to anticipate these concerns, and the evaluation of criminal aspects associated with the type of predicate offences, at the intelligence and analysis stage where FIUs' cooperation lies.

Existence of criminal investigations or legal proceedings

FIUs are often also prevented from providing the prior consent in cases where criminal investigations or legal proceedings are ongoing on the same or related cases in their countries.

The consent in these cases may be conditioned to authorizations released by law enforcement agencies or competent prosecutors. Authorizations may be decided upon on a case-by-case basis and are largely discretional, depending on whether or not the authorizing authority believes that the ongoing investigations or prosecution might be jeopardized or that the police or judicial cooperation channels should rather be used, instead of the FIUs' cooperation channels.

Limitations and conditions to FIUs' cooperation associated with the existence of investigations or legal proceedings are not in line with the provisions in the Directive. The extent of these undue derogations appears particularly broad with potentially significant implications on the FIUs' capacity to provide inputs to domestic investigations on money laundering and terrorist financing cases through the dissemination of information received from foreign counterparts.

Impairment of a criminal investigation

As allowed by the Directive, the vast majority of respondents have indicated that the consent cannot be provided, or is subject to conditions or limitations, when the requested use or dissemination is likely to cause the impairment of domestic ongoing investigations. The conditions and limitations that respondents are subject to are mostly related to the need to obtain ad-hoc authorizations by a competent law enforcement agency or a prosecuting magistrate.

Although responses to the Survey have not flagged this concern specifically, FIUs may not be aware of criminal investigations ongoing in their jurisdictions on cases or subjects involved in a request for assistance received from a foreign FIU. Even in cases where they happen to know that relevant investigations are underway, FIUs may not be in a position to determine whether granting the consent to a foreign counterpart to further use or disseminate the information exchanged is likely to impair such investigations. Because of this, there is a risk that, any time that the FIU is aware of ongoing investigations it simply refrains from providing the consent, using its discretion to avoid any possible risk of impairment.

Suitable mechanisms should be established at the national level to allow the FIU to become aware of investigations possibly linked with international exchanges and evaluate if granting a consent could jeopardise such investigations. In any event, the FIU (and its staff) should be protected from any possible undue responsibility; it should also be clear that the decision to grant the consent is taken by the FIU based on the information it has or can obtain.

Clarifications on these points could be provided through EU provisions, so as to allow unequivocal and uniform national implementation.

Disproportion with legitimate interests; contrast with fundamental principles of national law

The vast majority of EU FIUs are allowed or compelled to refuse the consent when the requested use or dissemination would be disproportionate with respect to "legitimate interests" of natural or legal persons or would be against "fundamental principles" of domestic law. As in other areas, the provisions on this point in article 52(2) of the Directive are quite general, leaving the interpretation of the notions of "legitimate interest" and "fundamental principle" entirely open to Member States and to FIUs. This is reflected in a particularly broad scope of application of these general clauses in national legal frameworks and on a considerably diversified understanding of instances that would fall into this scope across different countries and FIUs.

Tax-related cases or information

Responses to the Survey show that significant limitations to the FIUs' capacity to grant the prior consent continue to exist when the case or the requested further use or dissemination may relate to tax matters or involve tax information.

Given that tax offences are recurring predicate crimes in significant money laundering cases across EU Member States, the "fiscal excuse" should not be allowed as a derogation to FIUs' cooperation obligations. Current provisions in the Directive (according to which "differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU", "to the greatest extent possible under national law") should be clarified and reinforced to include a straightforward prohibition to refuse cooperation through consent for pursuing tax-related money laundering cases.

The FATF standards should be recalled on this point: the Interpretive Note to Recommendation 40 explicitly prohibits refusals to provide assistance "on the grounds that (…) the request is also considered to involve fiscal matters".

Conclusions and proposals

Based on the overview and analysis conducted, the EU FIUs' capacity to provide the consent to foreign counterparts to disseminate their information for use in criminal investigations or proceedings (or, more broadly, to disseminate their information to law enforcement bodies or prosecutors) is significantly impaired, particularly when:

- the predicate crime is not identified in the request or not criminalized in the Country of the requested FIU or, in some cases, when it is a tax offence (conditions of "double criminality" and "fiscal excuse");
- regardless of the type and nature of the possible underlying criminality, there are investigations or legal proceedings underway on the same cases in the country of the requested FIU.

While these conditions typically apply in the context of Mutual Legal Assistance forms of cooperation, they should not play a role at the prior stage of FIUs' cooperation. Differently from law enforcement agencies that are involved in the investigation of specific offences, FIUs deal with the analysis of suspicious facts and are not normally in a position to assess if crimes are being or have been committed and, even more, what is their type or nature. Requiring FIUs to assess the possible underlying criminality, based on their analysis, and making the consent (and the dissemination that depends on it) subject to this assessment deprives law enforcement bodies and prosecutors in the Country of the requesting FIU of relevant information, to the detriment of the effectiveness of the FIUs' dissemination for pursuing crimes.

Re-casting cases of derogation to the consent

Appropriate measures and initiatives should be devised to address these problems. The general provisions in article 55(2) of the fourth Directive about cases where the consent can be refused should be better detailed and specified. These cases should be reasonably narrowed down, so as not to overturn the general obligation to provide the consent to the largest extent possible. Cases for refusing or limiting the consent should be confined to instances where an ongoing investigation could be seriously impaired in the country of the requested FIU or the information is to be used by prosecutors or judicial authorities as evidence in the context of legal proceedings.

Consenting the dissemination to law enforcement agencies and prosecutors, not the use as evidence

However, it is the use of the information for evidentiary purpose that could be refused by the providing FIU on the ground that this use should be made subject to the activation of the appropriate MLA mechanisms and to the conditions applicable in this context (including about possible dual criminality requirements). The dissemination of the information exchanged between FIUs should in any case be possible (and thus authorised through the consent) precisely with the aim to allow competent law enforcement agencies or prosecutors to trigger MLA requests for the use of that information for evidentiary purposes.

Making the information available to law enforcement or prosecutors conducting a legal proceeding would be instrumental to allowing these bodies to consider undertaking MLA initiatives, to which the use of the information as evidence would still remain subject. Consistently, the consent for the dissemination would be given by FIUs in such cases under the condition that the information will be used solely for MLA purposes and is not to be used directly as evidentiary material in the context of the ongoing legal proceeding.

By allowing dissemination of FIUs' information to law enforcement or judicial bodies, regardless of the indication and evaluation of the type of possible crimes involved, these bodies would be put in a position to assess its relevance and, when appropriate, file proper MLA requests for using that

information in particular legal proceedings. Only at this stage, in accordance with the legal regime applicable to police and judicial cooperation, the indication of the crime and its type becomes relevant.
This approach would thus ensure that FIU-to-FIU cooperation, devoted to analysis of suspicious transactions (and to the inherent dissemination), is not obstructed at the dissemination phase and is not frustrated in its basic purpose, which is precisely to provide support to ensuing investigations and prosecutions by adding value through intelligence based also on meaningful foreign information. At the same time, all evaluations on the possible use of the information for evidentiary purposes would be in no way prejudged in the subsequent stage of police or judicial cooperation, which would always have to be triggered for this purpose.
Some practical difficulties need to be carefully considered and tackled through appropriate measures. These difficulties are related to the absence, to date, of safeguards and clear and binding legal provisions which ensure that FIUs' information passed on to law enforcement agencies or prosecutors is not improperly used as evidentiary material in a legal proceeding without duly triggering a prior MLA initiative. In fact, it may well be that, in the absence of explicit provisions on this matter in domestic or EU legislation, neither the terms of the foreign FIU's consent nor the limitations stemming from it as specified by the domestic FIU are binding upon the law enforcement bodies or the prosecutors receiving the information.
Police agencies and magistrates may well be allowed, or even required, to use any information that becomes available as a means to build the evidence necessary in support of the investigation, even regardless of the source of the information and of the possible conditions attached to its use, in the different FIU-to-FIU cooperation context. The prosecutors and judges would simply be a third party with respect to the FIUs' agreement about the consent and the attached limitations and not bound by them.
The absence of safeguards and limitations to the use of foreign FIUs' information in legal proceedings in conformity with the terms of the consent is certainly a strong deterrent for FIUs to grant the consent in the first place. Respondents have flagged these concerns in their submissions.

Use and dissemination for intelligence purposes
Use and dissemination for intelligence purposes, also in the context of subsequent investigations, should in principle always be possible. The dissemination for such further "intelligence purposes" should be considered as strictly inherent to the general dissemination function of FIUs and should follow as a natural consequence of the initial exchange.
In fact, the sharing of information and the analysis function are instrumental to dissemination; more specifically, analysis not followed by the dissemination of their positive outcomes, supported by either domestic or foreign information, is meaningless. For these reasons, the consent for the ordinary dissemination by the FIU for further intelligence should be presumed as implicit in the provision of the information through FIU-to-FIU cooperation. Rather than a "prior consent", the possibility should be envisaged to deny the further use and dissemination for intelligence purposes in limited exceptional circumstances. Based on developing practices, appropriate provisions to this end could be set at the EU level.

7. Cooperation with non-FIU counterparts ("diagonal cooperation")

Features, modalities, difficulties

Besides the exchange of information among themselves, FIUs (like other authorities) can be called on to cooperate with foreign agencies that are not FIUs. For what concerns FIUs, forms of "diagonal" cooperation with foreign agencies that exercise different functions are pursued

particularly in cases where either the functions of these latter agencies can receive support from STR/SAR information or, vice versa, when the FIUs' analytical activities to uncover money laundering, predicate offences or terrorist financing can benefit from information held by foreign non-counterparts. In this perspective, forms of diagonal cooperation between FIUs and foreign non-counterparts can be particularly useful to pursue investigations or supervisory actions, as well as to invigorate and further substantiate the FIUs' analyses taking account not only of law enforcement or supervisory information ordinarily available through domestic cooperation but also of information of the same nature held by foreign agencies.
On the other hand, it is also important to bear in mind that FIUs' information on STRs/SARs and their analysis is particularly sensitive and should be adequately protected against too extensive uses via excessively broad forms of diagonal exchanges with foreign non-FIU agencies.
Diagonal cooperation can be carried out according to different modalities and through different channels.
The vast majority of EU FIUs that can engage in international diagonal cooperation with foreign non-FIU counterparts do so through indirect means, that is through the FIU-to-FIU mechanisms. These are cases where STR/SAR information are first transmitted to the FIU of the country where the interested non-counterpart is located and then forwarded to such non-counterpart, based on the
Despite diagonal cooperation being increasingly practiced by FIUs and other competent authorities, it appears to be still under-utilised and subject to significant difficulties and uncertainties. This may also depend on existing different approaches and conditions across Member States which, in turn, depend on the lack of a uniform common framework at the EU level. In fact, while the 2012 FATF Recommendations have introduced a requirement to permit indirect diagonal cooperation, the fourth Directive neither foresees nor regulates international diagonal cooperation for AML/CFT purposes.
The Survey and the analysis conducted have highlighted several outstanding issues surrounding the capacity of EU FIUs to carry out diagonal cooperation. These issues appear to require appropriate regulation on some key aspects to be adequately tackled. This regulation should be implemented at national level against a uniform background at the EU level to ensure that common approaches are followed and effectiveness is achieved.

Lack of appropriate legal basis
First of all, diagonal cooperation frequently lacks a legal basis in EU Countries. This entails that, while several FIUs lack the capacity to engage in this form of cooperation entirely, others can share information with non-counterparts either based on implicit assumptions based on their domestic legal framework or utilising the same provisions applicable to FIU-to-FIU cooperation and adapted to accommodate forms indirect diagonal sharing based on an "ad-hoc" consent following the initial sharing. In both cases, diagonal cooperation rests on uncertain grounds and finds significant constraints stemming most of all from the lack of capacity for many FIUs to allow the use of the STR/SAR information provided for purposes other than analysis or investigation (e.g. supervisory actions) or for the ascertainment of criminal activities other than money laundering or terrorist financing.
In this context, while in principle nothing seems to prevent FIUs from requesting foreign non-counterparts for information useful for the analyses of the former, the FIUs' capacity to contribute to other authorities' activities which could benefit from STR/SAR information appears limited. More particularly, due to its narrow scope, diagonal cooperation cannot be pursued in many cases (at least, not systematically) in support of law enforcement activities (especially in relation to investigations or prosecutions not related to money laundering or terrorist financing), fiscal purposes or supervisory actions carried out by competent authorities in other countries.
Of course, it is important to ensure that sensible STR/SAR information is not overly exposed and unduly or excessively divulged through indiscriminate inter-agency sharing (both domestically and internationally). Nonetheless, in the current state of affairs, due to uncertain or inadequate legal

bases, it seems that the potential of diagonal cooperation for FIUs to uncover criminal or anomalous activities related, but additional, to money laundering or terrorist financing remains significantly unexploited and these forms of international cooperation are substantially under-utilised.

Direct and indirect channels for diagonal exchanges and involvement of interested FIUs

Differences in the forms and modalities through which diagonal cooperation is carried out by the FIUs that have the capacity to do so represent another significant obstacle to the development of the exchange of information with foreign non-counterparts.

While several FIUs can only provide information diagonally through indirect transmission to the FIU of the country concerned, a significant number of them can instead liaise directly with foreign non-counterparts, which raises the issue of lack of communication with the FIU of the country concerned, especially important when STR/SAR information is transmitted. Even in cases of indirect diagonal cooperation, there seems to be no indication on whether the information should be passed on to the final recipient through the local FIU or through other authorities, domestic or foreign.

Also due to the different forms and procedures used for diagonal cooperation, an issue of security and adequate protection of STR/SAR information has to be flagged. Outside of the FIU-to-FIU communication networks there are no guarantees that appropriate and commensurate safeguards are applied to the circulation of STR/SAR information. As diagonal cooperation can be carried out by means of direct communication with foreign non-FIU counterparts or through agencies that are not FIUs, risks of inadequate data secrecy and protection in the transmission also play a significant role as a deterrent to diagonal cooperation.

Direct "diagonal" exchange of police information

Cases of direct transmission of information to foreign non-FIU counterparts are currently reported by police FIUs which exchange information with law enforcement agencies in other countries, specifically through the police international cooperation mechanisms. To the extent that the information exchanged derives from STR/SAR or concern suspicious money laundering or terrorist financing activities, the question arises of whether in these cases the exchange should be carried out in the context of the FIU-to-FIU cooperation, rather than through law enforcement cooperation channels. There is also a risk that, as also discussed in relation to the FIUs' analysis function and cooperation, the necessary distinction between FIUs' activities and cooperation and law enforcement activities becomes blurred, with the former being absorbed into the latter.

Possible measures

The setting up of a uniform legal framework at the EU level on some key points, in line with FATF and Egmont standards on the same matters, appears necessary.

There should be a requirement for Member States to empower FIUs to exchange information with non-FIU counterparts from other Member States for appropriate purposes. These should include, in addition to preventing and detecting money laundering, predicate offences and terrorist financing through intelligence, the support to law enforcement activities, fiscal controls, supervisory actions (thus enlarging the current "purpose limitation").

In line with international standards, diagonal information sharing between FIUs and other "eligible" foreign agencies should be possible but not mandatory, contrary to the FIU-to-FIU exchange.

Also to compensate for the wider scope of international information sharing resulting from the derogation to the "purpose limitation", conditions limiting the exchange could be explicitly mentioned (in addition to the discretionary nature of diagonal exchanges), such as those about reciprocity (foreign non-FIU agencies should in turn be able to send information to FIUs upon their requests).

Appropriate and uniform modalities and channels should be set out for carrying out diagonal cooperation under a regime common to all EU FIUs. In this context, the use of secure

communication channels for the transmission of STR/SAR information, typically those in use for the FIU-to-FIU cooperation, should be required.
With a view to allowing for secure communication channels and ensuring that all interested FIUs are involved and duly informed about diagonal exchanges concerning potential money laundering or terrorist financing cases relevant to their countries, diagonal exchanges should take place indirectly, through the FIUs of the countries involved. In case of direct diagonal sharing, should these be allowed, while requiring that FIU-to-FIU cooperation mechanisms are not replaced by law enforcement channels, there should be a requirement to inform in all cases the FIUs of the countries concerned.

8. Data protection, confidentiality, security

The responses to the survey suggest that EU FIUs have rules in place governing the security and confidentiality of information and procedures for handling, storage, dissemination, protection of, and access to, information. Respondents indicate that FIU staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. All FIUs also informed that there is limited access to their facilities and information, including information technology systems.
Taking into account information provided by financial intelligence units regarding data protection, security and safeguards at the organizational level, it seems that Member States and EU FIUs have put in place strong and comprehensive measures in line with FATF standards in this area. FIUs have referred to various solutions, in particular limiting access to FIU premises, IT systems and data along with safeguards associated with personnel.
Nevertheless, an analysis of information security and confidentiality safeguards regarding the FIU work cycle reveals significant differences in how information is received, obtained, processed or otherwise handled while performing the FIUs' core functions and how it can be shared or communicated, either within the FIU, with domestic third parties or with foreign counterparts. Based on responses, this "legal" aspect seems to be less uniform and less regulated across the EU then the aforementioned organizational safeguards. EU FIUs are subject to differing confidentiality regimes, based on domestic legislations, determining how the information should be processed and kept confidential in the exercise of their core functions.
It is important to underline, that differences in data protection, security and confidentiality measures maintained by EU FIUs can have a negative influence on the capacity of these units to exchange information with each other.
To address the issues posed by uneven safeguards on information across Member States and FIUs a more robust, comprehensive and uniform legal basis at the EU level regarding data protection, security and confidentiality safeguards may need to be considered.

9. Most relevant problems encountered in FIU-to-FIU cooperation

The survey on shortcomings that affect EU FIUs' activities, powers and cooperation, has been conducted in the previous chapters on the basis of information provided by respondents on discrete, pre-identified issues and on the analysis conducted on such information. Under this "bottom up" approach, the survey attempts to identify existing problems and their root causes by mapping FIUs' features and activities, comparing them with what is required by relevant EU provisions and international standards and elaborate on the adequacy and effectiveness of FIUs' action in key areas.

This analysis has been complemented by an overview of inputs and comments provided by EU FIUs on the most prominent problem areas where they experience difficulties in conducting effective cooperation activities and where they think that improvements should be realised in the EU framework. The problems mentioned and the comments provided by FIUs, based on their direct operational experience, match significantly the findings emerging from the analysis conducted.

EU FIUs have consistently referred to, as the most relevant obstacles that still limit the effectiveness of cooperation within the EU, issues related to, i.a.: differences in FIUs' status and powers; refusals based on the need for prior STRs/SARs or to existence of investigations or to the need to use law enforcement cooperation channels; lack of cooperation due the identification and type of underlying offences; insufficient capacity to obtain and share information (particularly as regards banking data and information in external databases or by obliged entities); insufficient capacity to provide consent for further use or dissemination of the information exchanged; lack of adequate motivation in requests; inadequate cooperation in cross-border cases; delays in providing feedback; difficulties in cooperating for postponing operations; increase in workload; absence of reciprocity.

CHAPTER 1

FIUs' DOMESTIC STATUS AND ORGANIZATION

1. Introduction

In line with international standards set by the FATF and the Egmont Group, article 32 of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter referred to as the 'Directive' or '4AMLD') provides for an obligation for Member States "to establish an FIU", a unit whose mandate is to "detect and effectively combat money laundering and terrorist financing". The Directive also envisages a definition of "FIU" (along the lines of that provided for by international standards), setting out the essential functions that it carries out in order to pursue its general mandate and outlines a few elements concerning FIUs' organisation, status, available information, resources. The Directive also deals with powers that FIUs have to be endowed with in order to effectively perform their functions and require that, for the same purpose, FIUs must be able to engage in several forms of cooperation among them, particularly by exchanging information (FIUs' powers will be discussed more specifically in Chapters 3 and 4, while Chapter 6 is dedicated to FIUs' cooperation).

Functions. The definition of "FIU" foresees that it is responsible for performing three essential tasks, bundled together in a unique and integrated sequence: a) receiving suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing; b) analysing these reports and other information; c) disseminating the results of its analyses and any additional relevant information to the competent domestic authorities, "when there are grounds to suspect money laundering, associated predicate offences or terrorist financing". Cooperation and exchange information, in support of the analysis activity, is also a core function of FIUs. They must have this capacity in compliance with EU law (see article 53 of the Directive) and international standards.

The combined exercise of these functions together makes the FIUs specialised units and, due to the peculiar nature and purpose of such functions, differentiates them from other national agencies operating in the same or closely related areas. For example, analysis on suspicious money laundering or terrorist financing transactions is inherently different from investigation and prosecution (of the same phenomena) as well as from supervision or oversight of compliance by obliged entities with AML/CFT obligations.

This consideration becomes particularly important when the FIU's functions are allocated to organisations that also perform other, more or less related, activities (as mentioned below, in fact, the organisational set up is flexible and left up to Member States). For example, police

organisations need to keep the FIU's functions separate from law enforcement activities in the same AML/CFT domain[17]; similarly, administrative agencies that perform, for example, supervisory tasks or fiscal controls have to ensure that the FIU's activities are organisationally separate from these tasks or controls.

Organisation. The Directive only refers to few essential elements that have to be fulfilled, strictly related to the peculiar functions assigned, leaving to the discretion of Member States the articulation of more detailed aspects, based on national specificities. Importantly, the task of receiving STRs/SARs filed by obliged entities established on the national territory, with the associated analysis and dissemination of results, requires that the FIU has to be set up as a central national body: there can only be one FIU in each country, centralising all information which derive from disclosures, performing analysis taking account of all this information and disseminating consistent outcomes. This is made explicit in article 32 which, in line again with international standards, refers to the FIU as a "central national unit".

The requirement to centralise all functions and powers into one national unit does not prevent FIUs from implementing forms of decentralised organisation and activity. For example, especially in countries with extensive territories or considerably broad reporting sectors, an articulation of branches at local level may facilitate the receipt and collection of information and may benefit analysis based on a closer consideration of local circumstances. At the same time, however, it is necessary that all decision-making processes and all available information remain centralised, so as to ensure comprehensive and consistent analysis and dissemination (as well as to allow meaningful cooperation with other domestic authorities and with foreign FIUs.). The challenge of keeping the FIU as a fully centralised national agency while allowing for some forms of decentralised activities at the local level may be particularly relevant for countries that have a federal or regional structure or in cases where the centralised FIU is located within a bigger organisation that has a territorial reach.

Status and independence. Provided that the FIU's functions are kept separate as specialised activities with respect to other activities entrusted to the same organisation and that these functions are exercised in a centralised manner at the national level, countries are free to choose the status and institutional setting which is deemed most apt for their respective FIUs. These can be set up either as stand-alone agencies or as units embedded in bigger organisations (as is most often the case).They can be given an administrative, a law enforcement or a judicial status, or a combination of those, depending on the nature of the organisation that hosts the FIU or otherwise provides its budget and other resources.

The Directive allows for flexibility as regards the FIUs' status but not for its functions. These cannot remain the same and must be kept distinct and separate from any other regardless of whether the FIU is set up as an administrative or a law enforcement body or as a combination of different components[18]. Again, it is important to underscore that the flexibility granted to Member States in defining the FIUs' organisation has to go together with a rigorous separation of the specialised functions of receiving, authorising and disseminating; these cannot be merged or commingled into the organisation or functions of the bigger host agency.

[17] On this, see specifically paragraph 2.

[18] The condition of flexibility on the choice of the FIU's organization and institutional status and the associated requirement that the assigned functions do not change in relation to such status are expressed in article 32 of the Directive, which as said focuses on what the FIU's tasks consist in without preempting in any way the organizational features and, even more explicitly, in article 52 in the area of FIU-to-FIU cooperation (which is also an essential mandatory function for FIUs): FIUs should in fact be able to cooperate "regardless of their operational status".

The Directive (as well as the international standards) goes one step further to ensure an effective separation by requiring that FIUs should be "operationally independent and autonomous" (article 32), which means that "the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information". This requirement of operational independence and autonomy applies to FIUs' and their functions also with respect to the bigger organization where FIUs may be hosted (see Chapter 2).

"Multidisciplinarity" of information and resources. Another requirement that limits the flexibility given to Member States in shaping the FIU's institutional setting is that, whatever the organizational model and features of the FIUs, these have to have access to "the financial, administrative and law enforcement information that they require to fulfil their tasks properly"[19]. Once again, the choice of the model cannot influence the capacity of the FIU to have access ("directly or indirectly, in a timely manner") to multidisciplinary information. Notably, this means that, for example, administrative FIUs should be able to access law enforcement information and law enforcement FIUs should be able to access financial and administrative information.

A condition that must also be fulfilled by Member States, under whichever institutional model chosen for the FIU, is that it must be provided with "adequate financial, human and technical resources in order to fulfil their tasks". Clearly, assigned resources must be dedicated to the FIUs' functions and, while they are normally provided by the host organization, they cannot be shared with the latter.

In essence, therefore, the Directive envisages a flexible framework for Member States to set up and shape their FIUs, as regards particularly the status and internal organization. At the same time, some mandatory elements are also established for FIUs, particularly as regards their functions, the independence and autonomy conditions, the adequacy of resources, and the availability of multidisciplinary information. As illustrated in the following paragraphs, this mixed approach of "constrained" flexibility has resulted, on the one hand, in considerably different solutions adopted by Member States for their FIUs; these are significantly diverse from each other as regards their nature, the host organization, the internal features, powers and procedures. On the other hand, despite the Directive establishing some common mandatory elements, these are often only referred to in general terms and, as a result, significant differences exist among FIUs in their activities and capacities.

For example, analytical functions (mentioned in the Directive but not further defined or described) differ in many cases in their scope and purposes, especially as regards the relations with law enforcement activities and the focus on underlying criminality as opposed to mere suspicions or financial anomalies. Available sources of information also vary considerably across Member States, with persistent constraints to FIUs' access depending on their status, in a framework where "financial, administrative and law enforcement data" is not further defined in the Directive and is therefore interpreted differently at national level. Also, FIUs' capacity to cooperate among themselves continues to encounter limitations and conditions deriving from both the lack of access to certain information and the lack of full capacity to exchange.

[19] It is important to recall that these "tasks" include both the domestic functions of receipt, analysis and dissemination and the cooperation through the exchange of information with other FIUs. The "multidisciplinary" requirement to exchange financial, administrative and law enforcement information with foreign counterparts is explicitly mentioned in article 4 of Council Decision 2000/642/JHA.

Against this background, and based on the outcomes of the survey, consideration should be given to the current level of harmonisation of EU provisions concerning FIUs. The ample flexibility allowed, especially on domestic aspects, may cause many discrepancies which in turn impact on FIUs' effective operations and cooperation.

2. Institutional setting - Nature of the FIU and organisation where it is located

Although with many nuances that make each national solution unique in its specificities, the EU FIUs can be grouped under three sufficiently homogenous "models", as regards their institutional nature and organization: administrative, law enforcement (or judicial) and "hybrid".

It is important to underscore that the identification of these different institutional models is purely conventional and the distribution of EU FIUs among them is somewhat arbitrary[20]. Each FIU maintains in fact its distinctive peculiarities, even within each category. For example, the Latvian FIU is labelled as an administrative body but, similarly to law enforcement FIUs, is linked to the Prosecutor's Office; the Cyprus and the Danish FIUs describe themselves as hybrid Units while being located in central police or judicial organizations in their respective Countries. The distinctions among FIUs based on institutional "models" are therefore often blurred and their importance should not be overestimated besides the benefits it brings for descriptive purposes.

However, it is also important to note that, regardless of the institutional model of choice, in some cases different organizations are involved in the governance of the EU FIUs (e.g., in the case of the Belgian FIU, the Ministries of Justice and Finance exercise a budgetary control, besides receiving annual reports by the FIU) and, also, that the staff is composed of personnel coming from multiple organizations (for example, the staff of the Belgian FIU includes officers from the police and from customs services, the staff of the Spanish FIUs includes police officers and that of the Cyprus FIU comprises officials from judicial, police and administrative entities).

EU FIUs are all set up within bigger host organisations, which in most cases provide the logistics, the budget and other resources. There is one notable exception of an FIU that has indicated that it is an autonomous entity, not embedded within another institution. Although the survey is not conclusive on this aspect, it seems that FIUs do not normally have their own legal personality (as they are part of a bigger legal person or public entity where they are located)[21]. The tables included in the following paragraphs provide an overview of the distribution of EU FIUs across these different institutional models, as well as of the organizations where they are located, based on the indications given by respondents.

The vast majority of respondents have indicated that there are no plans in their respective Countries to change the FIUs' status and institutional setting in future legislative reforms, particularly in the context of the implementation of the fourth Directive. An FIU has indicated that forthcoming reforms are foreseen which will change its status from "law enforcement" to "administrative" and that the Unit will be moved from the national police organisation to the Ministry of Finance. Another respondent has referred to plans under implementation aimed at making the FIU, which is currently located within the Ministry of Finance, an independent and stand-alone unit. Other respondents have anticipated reforms which will confer additional tasks to the FIU (namely in the

[20] The repartition of EU FIUs across the identified models is based, in this report, on the responses provided by the FIUs themselves to the Survey and on their own evaluation about their nature.

[21] Some FIUs, however, may have legal personality. This is the case, for example, of the Romanian and of the Belgian FIUs. This latter (CTIF/CFI) is set up with its own legal personality while being under the joint supervision of the Ministries of Justice and Finance.

area of supervision of compliance with AML/CFT obligations) or will improve the internal organisation as regards human resources, technical tools and procedures.

2.1 Administrative FIUs

Twelve EU FIUs have indicated that they have an administrative nature. These FIUs are located, often as specialised and autonomous units or departments, into the ministries of Finance, Justice or Interior. Others are embedded into the Central Bank or a supervisory authority.

Such an FIU may be seen in the case of the Italian FIU, set up as an independent and autonomous Unit within the Bank of Italy, based on the law and on an ad-hoc regulation which implements the independence conditions and ensure appropriate coordination with other departments of the Bank.

The Spanish FIU is also established by the Central Bank (that provides the resources) and is attached organically and functionally to the Commission for the Prevention of Money Laundering and Monetary Offences, an inter-agency body which, through its Standing Committee, provides ongoing guidance for the FIU's action and approves its operating guidelines.

Administrative FIUs can also be located into a Prosecutor's Office, or belong to the organization of national security and information services. In one case, the FIU is set up as a stand-alone, autonomous and independent agency not embedded or established within another organisation.

ADMINISTRATIVE FIUs		
Member State	Denomination	Description
Belgium	Cellule de Traitement des Informations Financières / Cel voor Financiële Informatieverwerking (CTIF-CFI)	Subject to the budgetary control by the Minister of Finance and the Minister of Justice
Bulgaria	Financial Intelligence Directorate of the State Agency for National Security (FID-SANS)	Within the State Agency for National Security (SANS), a specialised body within the Council of Ministers for the protection of the national security.
Croatia	Anti-Money Laundering Office (AMLO)	Ministry of Finance of the Republic of Croatia
Czech Republic	Financní analytický útvar (FAU – CR)	Organizational part of the Ministry of Finance
France	Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN)	Ministry of Finances
Italy	Unità di Informazione Finanziaria per l'Italia	Established within the Bank of Italy as an autonomous and independent Unit.
Latvia	Kontroles dienests, Noziedîgi iegûto lîdzeklu legalizâcijas novçrsanas dienests (KD)	The FIU is an independent monitored by the Prosecutor's Office.
Malta	Financial Intelligence Analysis Unit - (FIAU)	Autonomous and independent body, not embedded within another organisation.
Poland	Generalny Inspektor Informacji Finansowej (GIIF)	Within the Ministry of Finance
Romania	Oficiul Nacional de Prevenire si Combatere a Spalarii Banilor (ONPCSB)	Specialized body and legal entity subordinated to the Government of Romania for administrative purposes.
Slovenia	Urad RS za Preprecevanje Pranja Denarja Ministrstvo za Finance Office for Money Laundering Prevention (OMLP)	Ministry of Finance
Spain	Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC)	Attached to the Commission for the Prevention of Money Laundering and Monetary Offences (CPMLMO), chaired by the Secretariat of State for the Economy

Table 1. Administrative FIUs by Member State

2.2 Law enforcement and judicial FIUs

Eleven respondents to the Survey have indicated that they are organised under a law enforcement "model". These FIUs are established in, or are part of, the respective national criminal police offices, agencies or services. They appear to be set up at different levels of the internal organisation, either as separate units (with own forms of governance) or as internal offices of law enforcement structures competent for fighting economic crimes or other serious crimes.

For example, the FIU of the Slovak Republic is set up as an independent unit within the National Criminal Agency of Police Force Presidium, a body focused on fighting against financial criminal activity, corrupt practices, serious crimes and other forms of crimes. The Head of the FIU reports to the Head of the NCA who in turn is responsible vis-à-vis the Minister of Interior.

The Swedish FIU is set up as an integrated body within the Swedish Police Authority. It specifically responds to the National Operations Department (NOA), a central body in charge of investigations and preventive work against financial crime and money laundering. The FIU's duties and functions are defined in internal guidelines, i.e. the Procedures for the Police Authority and the Process for NOA.

In one case, the FIU is articulated in a central structure at the federal level and several territorial branches at the state level (primarily responsible for the operational analysis of STRs). One FIU has indicated that it adopts a judicial model: it is set up as a specialised unit within the Public Prosecutor Offices and its staff is composed mainly of prosecutors, who are in charge of the analytical work.

LAW ENFORCEMENT FIUs		
Member State	Denomination	Description
Austria	Bundeskriminalamt (A-FIU)	Criminal Intelligence Service Austria (Ministry of the Interior).
Estonia	Rahapesu Andmebüroo	Part of the Estonian Central Criminal Police of the Police and Border Guard Board.
Finland	RAP Keskusrikospoliisi / Rahanpesun selvittelykeskus	Part of the Criminal Intelligence Division which is part of the National Bureau of Investigation.
Germany	Zentralstelle für Verdachtsanzeigen	The FIU Germany is part of the federal criminal police office.
Ireland	An Garda Síochána / Bureau of Fraud Investigation (MLIU)	The Irish FIU is situated within An Garda Siochana, the National Police Force in the Republic of Ireland
Lithuania	Finansiniu Nusikaltimu Tyrimo Tarnyba Prie Lietuvos Respublikos Vidaus Reikalu Ministerijos Pinigu Plovimo Prevencijos Skyrius	Established under the Ministry of Interior.
Portugal	Unidade de Informaçao Financeira	Body within the Judicial Police
Slovak Republic	Finančná spravodajská jednotka národnej kriminálnej agentúry Prezídia Policajného zboru (FSJ Slovakia)	Independent unit within the National Criminal Agency, a specialized Section of the Police Force Presidium for the fight against financial crimes, corruption. Serious organized crimes and drug crimes
Sweden	Finanspolisen (FIPO)	Set up within the National Operations Department of the Swedish Police.
United Kingdom	National Crime Agency (NCA)	Within the National Crime Agency (NCA), leading UK Law Enforcement's fight to cut serious and organised crime.

Table 2 – Law enforcement FIUs by Member State

JUDICIAL FIU		
Luxembourg	Cellule de Renseignement Financier (CRF)	Public Prosecutor's Office ("Parquet") of the Luxembourg district Court

Table 3 – Judicial FIU

2.3 "Hybrid" FIUs

Five respondents to the Survey have described themselves as having a "hybrid" nature, due to the combined presence of administrative and police elements. These FIUs are mostly located in national police offices or in the office of the attorney general or of the prosecutor, are separate from operational police or judicial units and are specifically dedicated to the analysis of suspicious transactions. The staff of hybrid FIUs often includes, in addition to law enforcement officers, analysts from other, non-police, organisations.

For example, the Hungarian FIU is set up as an autonomous department within the law enforcement branch of the National Tax and Customs Administration (NTCA). However, it is not involved in criminal investigations or legal proceedings and is not part of the investigative authority of the NTCA.

The FIU of Cyprus (MOKAS) is a multi-disciplinary Unit established within the structure of the Law Office of the Republic/Attorney General's Office. It is composed of officials from the Attorney General's Office, the Police, the Customs and Excise Department, as well as financial analysts.

The Hellenic FIU is set up as one of the three Units of the Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority (administratively and operationally independent). The FIU consists of the Head and eight board members.

HYBRID FIUs		
Member State	Denomination	Description
Cyprus	Unit for Combating Money Laundering (MOKAS)	MOKAS is a multi-disciplinary Unit established within the Law Office of the Republic/Attorney General's Office.
Denmark	SØK / Hvidvasksekretariatet Stadsadvokaten for Særlig Økonomisk Kriminalitet / Hvidvasksekretariatet (HVIDVASK)	Independent entity at the Special Prosecutor for Serious Economic and International Crime (SØIK).
Greece	Hellenic-FIU	Set up as one of the three Units (Unit A) of the Anti-Money Laundering, Counter-Terrorist Financing and Source of Funds Investigation Authority.
Hungary	NAV Központi Irányítás Pénzmosás Elleni Információs Iroda	Autonomous department within the National Tax and Customs Administration (NTCA).
Netherlands	Financial Intelligence Unit-The Netherlands	Located within the Dutch National Police.

Table 4 – Hybrid FIUs by Member State

2.4 Conclusions

Against a background of broad flexibility allowed by the Directive, EU FIUs are all different from each other, particularly as regards their status or nature, the internal organization and governance, the composition of the staff. Although some commonalities can certainly be identified, each

Member State has defined its unique and peculiar "blend" for its FIU. This results in a very varied and diversified landscape.

The diversity stems from the flexible approach adopted by provisions in EU law on organizational and institutional aspects, according to which these aspects may well vary provided that the activities, functions and powers of FIUs, as diverse as these institutions can be across the EU, duly correspond to the provisions in the Directive (thus also ensuring a certain level of uniformity). However, the replies to the Survey seems to suggest that differences in domestic characteristics are not irrelevant for the FIUs' workings, both internally and in reciprocal cooperation: they affect the status of autonomy and independence (see Chapter 2), the features of FIUs' functions (which, in turn, are only loosely described in the Directive, especially as regards "analysis"), the extent of their powers and information available, the modalities and conditions surrounding the activities carried out.

An area where the nature of the FIU can directly influence the nature of its functions and where, therefore, the flexibility allowed for the former implies that the latter may also change contrary to the paradigm which seems to underpin the provisions of the Directive[22], is that of the FIU's "analysis" of suspicious money laundering or terrorist financing cases. This function is not defined or described in details in the Directive[23]; in lack of a common notion towards which FIUs can converge, they conduct activities, all labelled as "analysis", which differ considerably in, i.a., scope, extent, information used, outputs and objectives.

Notably, these differences appear to depend crucially on the FIUs' institutional nature and context: police-type FIUs tend, in general, to carry out investigations based on STR/SAR material, thus merging analysis and law enforcement activities into a unique activity; on the other hand, administrative or hybrid FIUs are normally confined to an administrative area of function where they focus purely on an analytical work on the understanding of financial phenomena without direct police implications (these are left to competent law enforcement agencies which receive appropriate inputs through ensuing dissemination by the FIU).

Cases where the distinction between analysis and investigation is blurred and the two are commingled, with the former being absorbed in the latter in the FIU's activities are clearly identifiable based on information provided by respondent and in other available material (see the references to findings in FATF Mutual Evaluations in Chapter 5). In these cases, the lack of separation and autonomy of the analytical functions, besides being in contrast with EU provisions and international standards as recalled at the beginning of this Chapter, brings a number of interconnected consequences, particularly on: the type and range of information available to FIUs, both as regards the structure and content of disclosures receives and the powers to obtain additional information (this will be discussed in Chapter 3); the nature and objectives of the domestic activities performed (as will be illustrated in Chapter 5); the capacity to provide information and cooperation to foreign counterparts (see Chapter 6 on constraints and limitations to FIUs' cooperation deriving from the overlapping of "analysis" and law enforcement purposes).

All this clearly illustrates how, far from being neutral, the nature and status of FIUs have far-reaching consequences on their functions and powers, as well as on domestic and international activities. It appears that, contrary perhaps to the intended objectives pursued through the flexible approach to the institutional setting and domestic features, differences among FIUs significantly

[22] And of the international standards of the FATF and of the Egmont Group on the same matters.

[23] Which, as more amply discussed in Chapter 5, only sets out general provisions on objectives and modalities of "analysis" in article 32(8).

impact on their activities and cooperation. While it remains to be seen if the shortcomings in effectiveness and quality cooperation are compensated by the benefits of domestic flexibility, the objective of making FIUs' activities and cooperation more effective and uniform cannot be achieved without reflecting on the need for more convergence among national approaches to FIUs' domestic status and features[24].

The survey suggests that improvements in FIUs' capacity to cooperate and an increased convergence towards homogeneous functions (especially as regards those carried out under the label of "analysis") would require:

- more detailed provisions at the EU level on a number of aspects concerning FIUs' activities and powers;
- more uniformity in FIUs' domestic features and a corresponding reduction of flexibility to foster convergence across the EU on key aspects impacting on functions and cooperation.

3. Additional functions carried out by FIUs

In addition to the FIU "core" tasks (receipt, analysis, dissemination, international cooperation), FIUs can of course be entrusted with additional functions, based on domestic legislation and arrangements. The majority of respondents have indicated that they indeed perform a considerable variety of additional tasks. These range from law enforcement to supervisory activities, from regulatory to domestic coordination functions in AML/CFT related areas; FIUs may also play a role in the implementation of targeted financial sanctions and in providing training to the private sector or to public partners.

Supervising and sanctioning activities. Several respondents are in charge of supervisory or oversight activities aimed at verifying compliance by obliged entities with AML/CFT obligations. These competences vary significantly in scope: in some cases, the FIU is mandated to supervise certain categories of non-financial entities (AML/CFT supervision on credit and financial institutions is ordinarily encompassed in the general prudential supervisory regimes in place in EU Member States), such as real estate agents, dealers in previous metal and stones, accountants, tax advisors). In other cases, the FIU's mandate covers all obliged entities but is limited to the supervision on compliance with only certain AML/CFT measures (namely, those related to detection and reporting of suspicious transactions). As regards the tools and powers that FIUs can use, responses to the Survey indicate that supervisory activities can be exercised through either on-site inspections or off-site activities. In some cases the FIU, when identifies areas of possible non-compliance in the course of its activities, can request other competent authorities to perform targeted supervisory interventions. A respondent has reported that it is in charge of licensing certain categories of obliged entities for market-entry purposes. Some FIUs have indicated that they can act upon the detection of cases of non-compliance by issuing (administrative) sanctions or triggering and initiating the sanction procedure.

Law enforcement activities. Some respondents (FIUs that have a police status) have referred to the role they play in coordinating national investigative activities on money laundering cases and in providing assistance to other police units in these matters. Police FIUs also often participate in, and process, Europol and Interpol enquiries, Mutual Legal Assistance requests related to money

[24] On this point, it is important to recall the Commission "Action Plan to strengthen the fight against terrorism financing", adopted in February 2016 (COM(2016)50), which specifically recall that, "depending on the results of the mapping exercise, the Commission will decide on whether and which kind of measures are necessary to address differences in the organizational status of the FIUs".

laundering or terrorist financing and inbound and outbound requests for criminal asset tracing intelligence. Some FIUs act as the national Asset Recovery Office or closely cooperate with the domestic agency that is in charge of this function. A respondent has flagged that it can exercise powers to freeze assets (beyond the ordinary postponement powers exercised by FIUs) with the purpose of acting prior to a concrete crime having been established or a criminal investigation being initiated.

Regulatory activities. Some respondents have referred to the roles they play in preparing or adopting regulation, under various forms, on AML/CFT matters. Some FIUs participate in the preparation of national regulatory acts, by providing advice to competent authorities (including the Government or the Parliament). In several cases, the FIU is in charge of issuing by-laws, guidance or instructions; these are mostly related to matters such as: the content and procedure for reporting suspicious transactions; guidance on red-flag indicators or risk factors; Customer Due Diligence and record-keeping measures. Some FIUs are specifically entitled to put forward proposals to competent bodies for the adoption of AML/CFT regulation.

Targeted financial sanctions. Some respondents are involved in the application and enforcement at the national level of targeted financial sanctions regimes, particularly as regards the implementation of UN Security Council Resolutions and EU Regulations imposing freezing measures upon listed individuals and entities for purposes of fighting, i.a., the financing of terrorism and of the proliferation of weapons of mass destruction.

National coordination and risk assessment. Some respondents have mentioned the role they play in coordinating the AML/CFT activities carried out by national competent authorities, both for domestic purposes and for the participation in the activities of international for a (namely, in the context of the national delegations to the FATF or FSRBs). Other FIUs have recalled the contribution they are called on to provide to the preparation and update of the national risk assessment, based on the experience gained through the analysis (operational and strategic) of suspicious money laundering and terrorist financing cases.

Training. Some FIUs are specifically in charge of performing training activities on AML/CFT matters, to the benefit of obliged entities and their employees but also vis-à-vis government bodies.

It is necessary that an appropriate separation is ensured between the functions carried out by FIUs as such (that is, those making up their very definition: receipt, analysis, dissemination, plus international cooperation) and the other, additional tasks assigned to them. This separation should be implemented both through appropriate organizational settings (specifically by allocating different functions in different internal structures with separate staff and procedures) and by ensuring that the information collected and processed in the exercise of the FIU's functions (namely that deriving from STRs, analysis and cooperation) is kept confidential and is not unduly used for different purposes.

4. Resources

Article 32 of the Fourth Directive establishes that Member States "*shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks*". The overview that follows, based on responses to the Survey, focuses on the availability for FIUs of these various types of resources and on related constraints and conditions.

4.1 Human resources

Whilst the most staffed FIU has reported 300 employees[25] and the least staffed has indicated 13 persons, the average amount of human resources available to EU FIUs is 58. The majority of FIUs (21) are below this average, with 14 respondents reporting up to 30 employees. Three medium-sized FIUs (as far as human resources are concerned) have between 58 and 100 members of staff, while the 4 most endowed FIUs have in excess of 100 staff. For the majority of respondents, the biggest portion of the human resources available is dedicated to the performance of core functions associated with receipt of STRs/SARs, analysis, dissemination and international cooperation. However, significant amounts of these resources are also allocated to other tasks.

10 respondents report that 50% or more of the available staff is not employed on core FIU functions. Resources are in fact absorbed to a considerable extent by the other activities that are discharged by FIUs (see paragraph 3 above) and, to a lesser extent, by administrative and support activities. While one FIU indicates that all available human resources are involved in core functions, at the other extreme another respondent report that less than 9% of the staff is dedicated to receipt, analysis, dissemination and cooperation with foreign counterparts.

HUMAN RESOURCES			
Member State	**Overall Staff**	**Staff dedicated to "core" functions**	**Staff dedicated to "core" functions in %**
Austria	19	16	84%
Belgium	51	31	61%
Bulgaria	30	16	53%
Croatia	22	14	64%
Cyprus	21	16	76%
Czech Republic	45	30	67%
Denmark	17	10	59%
Estonia	16	6	38%
Finland	30	20	67%
France	124	92	74%
Germany	300	289	96%
Greece	30	17	57%
Hungary	36	23	64%
Ireland	13	5	38%
Italy	138	117	85%
Latvia	30	13	43%
Lithuania	21	10	48%
Luxembourg	14	8	57%
Malta	24	8	33%
Netherlands	57	50	87%
Poland	63	38	60%
Portugal	31	20	65%
Romania	104	49	47%
Slovak Republic	45	20	44%
Slovenia	20	9	45%
Spain	98	49	50%
Sweden	34	20	59%
United Kingdom	80	80	100%

Table 5. Human resources: Overall and dedicated to "core" functions (%)

[25] This respondent has an organization articulated in a central headquarter and local branches (decentralized police offices on the territory); the staff of these latter may not be dedicated solely to the FIU's activities.

These figures and statistics allow an insight into EU FIUs' dimension and organizational complexity. They are also useful to appreciate the extent to which core FIU functions absorb human resources and how these are distributed, in each EU FIU, between these functions and other, non "core", tasks equally assigned to FIUs. Of course, an assessment on the adequacy of available human resources, both in relation to each particular FIU and based on a comparison among differently staffed Units, would require an analysis of the respective workloads, particularly as regards the number of disclosures received, the type of the analyses and disseminations performed (specifically considering the FIU's approach towards selecting relevant cases and information[26]), the volume of international exchanges.

In any event several respondents highlight that the implementation of the fourth Directive, and the associated reforms brought about by domestic legislation, will entail the assignment to the FIU of additional functions or an increase in the workload, deriving particularly from analysis and dissemination of STRs/SARs and from FIU-to-FIU cooperation[27]. These respondents anticipate that an increase in available staff will be necessary to adequately cope with these additional tasks and workloads.

Some respondents have informed that the staff employed by the FIU includes personnel coming from or seconded by other domestic organisations[28]. In these instances it is important that the effective use and circulation of information within the FIU, across different categories of staff, do not result in this information being unduly shared with the organizations of origin of the personnel.

4.2 Financial resources

Only less than half of the EU FIUs have indicated that they dispose of an autonomous budget, that is an amount of funds assigned specifically (and exclusively) to them for expense coverage and managed independently. Seventeen Respondents have in fact indicated that, being part of bigger organisations, they draw the needed financial resources from those organisations, within the budget of these latters which is normally determined by the Parliament, in case of ministries, or by ministries, in case of separate organisations such as police bodies or judicial offices.

4.2.1 Lack of an autonomous budget

FIUs that lack an ad-hoc pre-assigned budget may also lack the capacity to manage independently the sums needed for their operational needs. However, this does not necessarily mean that the same FIUs lack operational independence or autonomy, that is, as far as financial resources are concerned, that they are unable to fund the expenses associated with their effective functioning. Several of these respondents, in fact, have indicated that they can obtain the necessary funding from the host organisation whenever this is needed to finance their operations. Access to financial resources on a need-to-have basis seems an adequate approach to secure the FIU's independent functioning, despite the absence of an autonomous pre-assigned budget. Problems may arise, in

[26] See article 32(3) and 32(8), where the FIUs' capacity to "select" cases and information in the analysis and dissemination tasks is recalled, and Chapter 5, where this point is discussed.

[27] Respondents flag particularly the expected impact deriving from the implementation of the provisions related to the reporting of "cross-border disclosures", in the context of FIU-to-FIU cooperation. This impact may vary depending also on the criteria that will be established for the identification of such "cross-border disclosures" (see Chapter …). The issue of the adequacy of the resources assigned to EU FIUs will also be dealt with in Chapter 2, in relation to the impacts on FIUs' autonomous and independent operations.

[28] See also considerations in Chapter 2, paragraphs 2.2.2 (specifically on the involvement of external staff in analytical activities) and. 3.

these circumstances, if the overall budget of the host organisation is limited, in such a way as it is not sufficient to support properly the needs of the FIU.

In situations where the FIU lack an autonomous budget the risk should be considered that, given that the overall budget of large and complex organisations (e.g. ministries) has of course to support multiple and diverse activities and entities within the general area of competence, the expenses needed and requested by the FIU do not feature sufficiently high in the overall list of priorities. In these cases of conflicting or overlapping priorities the objective of securing the adequate functioning of the FIU could be postponed with respect to other objectives that are considered more pressing, to the detriment of both the effective operations of the FIU and of its independent and autonomous management.

An additional risk is that, of course, the selection of priorities underpinning the allocation of available resources from the general budget is driven or influenced by political considerations (as is certainly possible in the management of budgets by ministries or other governmental authorities). While political considerations in spending matters are normally fully legitimate, when they impact on the functioning of the FIU its capacity to function independently may be affected. Especially in cases of significant cuts in spending, the FIU's effectiveness can be hindered.

On this aspect, it is important to recall that the FATF standards explicitly maintain that "the FIU should be able to obtain and deploy the resources needed to carry out its functions (…) free from any undue political, government or industry influence or interference, which might compromise its operational independence"[29].

Clearly, the same or similar issues may equally well arise in situations where the FIU does have an autonomous budget but the decision on the assignment of the budget and on its dimension is dependent on political considerations and, as a result, the available resources are not sufficient for the independent and effective functioning of the unit.

While, as said, some respondents to the Survey have clarified that, although they lack an autonomous budget, they do not encounter particular limitations in obtaining needed resources from the parent organization, it is not clear from responses if these resources are drawn from funds specifically earmarked to the FIU within the general budget (which would be similar to the FIU having a own dedicated budget) or if they are obtained only based on proven need and through ad-hoc procedures.

In this latter case, issues of independent decision-making may arise again, to the extent that the FIU's request for funding is made subject to particular scrutiny and conditions by competent offices in the host organization. In general, the existence of earmarked resources in the overall budget would seem to provide stronger safeguards with respect to the FIU's independence (provided of course that the assigned resources are adequate).

4.2.2 Autonomous budget

As regards the eleven respondents that have indicated that they possess autonomous budgets, for whose spending they are also responsible, the amount of available resources varies considerably, ranging between a minimum of 600.000 EUR and a maximum of above 14 million EUR on a yearly basis. The adequacy of these figures could of course only be assessed taking account of factors such

[29] Interpretive Note to Recommendation 29, par. 12. This element, however, like others mentioned in the FATF standards concerning FIUs' operational independence and autonomy, is not reflected in the fourth Directive.

as the dimension of the interested FIUs (which is clearly an important determinant for spending needs and also varies considerably across the EU), the spectrum and types of the tasks assigned, the magnitude of the workload and volume of the activities carried out.

Similarly to the arrangements applicable also to other FIUs, the autonomous budget is either assigned to these FIUs as part of the overall state budget (as determined, normally, by the Parliament) or is paid out by the competent host organization (ministries or other authorities or agencies). One respondent has indicated that its budget is financed by reporting entities.

Interestingly, while FIUs are in most cases exclusively dependent on external funding, a respondent has reported that it produces "a fixed annual income generated by [the FIU] through its supervisory functions". In addition, this FIU generates additional income which is variable (such as income from administrative penalties)". These sources of income accrue to the autonomous budget assigned by the Ministry of Finance.

A need to go through ad-hoc expenditure procedures as well as reporting and accounting duties is often associated with the management of an autonomous budget.

For example, a respondent has highlighted that the organization providing the budget (which in this case is different from the organization where the FIU is located) "shall draw up daily justified accounts" for "the expenses incurred under the budget approved" by the host organization, "which it shall refer to" the Ministry of Treasury. This Ministry, "after verifying said accounts, shall pay the amount" to the organization providing the budget, "charging against the non-budget item created for this purpose by the State Comptroller's Office".

4.2.3 "Mixed" approaches

In contrast to FIUs that either have dedicated budgets or can only obtain resources from the parent organization, some respondents have indicated that they operate under a mixed approach: while the bulk of the expenses is sustained by the host organization through its budget (e.g. staff salaries, IT and office equipment, costs of premises), these FIUs are also endowed with a (relatively limited) amount of financial resources which they can spend autonomously for particular purposes such as, for example, funding business trips, supporting participation in training initiatives, payment of membership fees in international organizations.

On this note, a respondent has clarified that "technical, logistic and human resources are directly assigned by the [host organization] to ensure the effective performance of the FIU and that "particular needs" that may arise in the course of operational activities are also "promptly satisfied" by the same organization. This is "in addition to the budget specifically earmarked" to the FIU which, although relatively limited in its amount (slightly less than 200.000 EUR in 2014), is managed directly and independently by the FIU.

4.3 IT resources

IT tools are essential for FIUs to manage and process effectively huge volumes of data associated with domestic functions (especially as regards the receipt and analysis of disclosures[30]) and with FIU-to-FIU cooperation. On this latter aspect, article 56(1) requires that FIUs "use protected channels of communication between themselves and encourage the use of the FIU.net or its

[30] See considerations on this in Chapter 3.

successor". Also, article 56(2) foresees that FIUs should "cooperate in the application of state-of-the art technologies".

The majority of the respondent FIUs believe they possess adequate IT tools dedicated to supporting the receipt, analysis, dissemination and international cooperation. In most cases, FIUs have developed in-house or ad-hoc IT systems in order to carry out their functions. A number of FIUs, instead, are using, or are planning to adopt, IT products offered by external providers (such as the "GoAML" package made available by the United Nations) and adjusted to fit into the FIUs' peculiar operational and procedural contexts.

Responses to the Survey also highlight that in many cases FIUs are considering to upgrade or to renew their IT equipment to respond to new functions or to the increased workload. In other cases, the FIU is in the process of developing projects in order to increase analytical capacity or to improve existing applications.

A respondent has indicated that it considers the available IT resources to be inadequate: possibilities to improve and develop the IT tools cannot be exploited because of the limited resources. In another case, an FIU has dedicated and adequate IT tools for dissemination and international cooperation, but lacks proper IT tools in support of STRs receipt and analytical functions; this FIU is planning to remedy these shortcomings through the GoAML software.

In general, a broader use of IT tools is indicated by respondents as a means to cope with the increasing workload by enhancing efficiency.

5. Governance

5.1 Internal organization - Organs and structure

Unsurprisingly, the internal organization of EU FIUs varies depending on the functions carried out and on their size. In some Countries FIUs are set up as relatively small units with very simple structures. In other cases, FIUs entrusted with multiple tasks, or facing bigger workloads, have more complex and articulated internal organizations, commensurate with the activities performed.

FIUs which are relatively small are characterised by a "flat" structure, composed of officers in charge of the same or similar analytical tasks. In some cases, respondents indicate that the basic sub-division of work is ensured by additional support units.

For example, a respondent has informed that its staff consists of 16 police officers. Each of them is assigned with the same tasks that include the receipt, analysis and dissemination of STRs, the lead of national investigations and the coordination of investigations taking place in the country.

Another FIU has informed that it maintains a core staff for inputting analysis and dissemination of STRs; also, there are two additional support Units dealing with money laundering and terrorist financing investigations.

Interestingly, especially in cases where the internal FIU's structure has a relatively simple articulation, respondents highlight that the work is distributed among staff coming from different organisations.

For example, a respondent has flagged that its staff is composed of officials from the Attorney General's Office, the Police, the Customs and Excise Department, as well as financial analysts and is headed by a representative of the Attorney General.

One respondent highlights that the FIU's organization is not divided into separate organs, but it works as a single entity under the direction of the Head of the FIU.

The structure of "bigger" FIUs is internally divided into areas or units, based on the distribution of analytical tasks (for example operational and strategic analyses are assigned to different internal units) or on a separation between analysis function and other support activities (e.g. legal, IT, human resources, internal audit, and others). Dedicated units are also normally set up within FIUs to deal with additional, non-"core", functions (this is typically the case of supervisory activities.

A respondent has indicated that, within its organization, the operational units are grouped under two directorates: one focused on the analysis of suspicious transactions and the other one in charge of the cooperation with the judicial authorities and other institutions, regulatory activities, international cooperation activities and analyses of aggregated financial flows. The two directorates are made up of a total of seven divisions. Recently two special bodies have been established: one within the Regulation and Institutional Relations Division, responsible for inspections, and one within the Information Management Division, responsible for STRs on terrorist financing and the money transfer sector.

Another FIU has described its internal structure as articulated into the following components: a) the President, appointed by the Government among the Members of the Board; b) the Board of the FIU, which includes representatives from several Ministries, the General Prosecutor's Office, the Central Bank, the Court of Accounts and the Banks' Association; c) the President's counsellors; d) General Operative Directorate, composed of: Analysis and Processing of Information Directorate; Information Technology and Statistics Directorate; e) Inter-institutional Cooperation and International Relations Directorate; f) Economic-Financial and Administrative Directorate; g) Supervision and Control Directorate; h) Legal and Methodology Directorate; i) Public Internal Audit Compartment; j) Human Resources Compartment.

For another respondent, the internal organization is articulated in 3 main areas: Analysis, Supervision and Obliged Entities. Under each of them there are several units with a separate Legal Unit. The Analysis area is articulated into several Units: "One composed of members of the competent police bodies; another one of the tax agency, two Units in charge of Analysis, one in charge of Strategic Analysis, and one in charge of International Cooperation".

One respondent highlights that its organization is articulated at a federal level and at a state level: the federal level is in charge of strategic and operational analysis, whilst the territorial branches at state level are primarily responsible for the operational analysis of STR. The information provided in the response does not provide confirmation that the exercise of core functions (receipt, analysis, dissemination), together with the access to related information, remains centralised.

When the staff working for the FIU comes from different organisations, this may pose issues of, i.a., confidentiality, direction, homogeneity of working methods. In these instances it is important that the external staff responds in full to the FIU's hierarchy, without having to report to the organization of origin, and is bound by the latter's internal procedures.

Organisations which have a federal configuration should ensure that all decision making processes

are kept centralised and that procedures and information are kept within the FIU.

Although organizations differ in complexity and models of task allocation, there are some commonalities. At the top of the FIUs' structure is in all cases a "Head" or "Director", variably denominated, and his/her deputy. Core functions are always assigned to internal units dedicated to the receipt and analysis of suspicious transaction reports and to strategic analysis tasks. As regards the exchange of information, this is sometimes assigned to the same analytical department, while, more frequently, it is entrusted to a separate department specifically responsible for international cooperation.

When a FIU also carries out supervisory and compliance functions, a dedicated department is normally established. In some FIUs specialised internal bodies have been also set up for the performance of inspective controls, anti-terrorist financing activities or of analyses focused on certain categories of obliged entities. In some cases, especially for bigger FIUs, support and secretarial functions are centralised and entrusted to a specialised internal unit.

In many FIUs, sophisticated data retrieval systems, storage and analysis technologies are in place, thus entailing the establishment of a dedicated IT department within the organization, or the assignment of specialist IT staff into the analysis department.

5.2 Appointment and removal of the Head of the FIU

The procedure for the appointment and removal of the FIUs' Head is of course a cornerstone of the FIUs' status of independence. On this point, differences among EU FIUs seem to depend crucially on the nature of the FIU and on the relations with the organisation within which it is located. Particularly important is the level of influence that this organisation can exercise on the embedded FIU, depending on how "deep" this embedment is and on the related participation in the decision-making process.

The appointment procedure is in almost all cases provided for by the national law or other regulations, which also set out the necessary requirements in terms of integrity and professional experience. The reasons for removal are often also established in law or regulation and generally refer to serious misconduct, infringements of laws, or failure to comply with the conditions required for the appointment. This certainly provides an adequate protection against potential undue influences, especially of a political nature.

One respondent, though, indicates that no formal procedure is provided for in domestic laws and that the Head of the FIU is appointed by the responsible officer of the parent organisation based on the direct consideration of candidates and their qualifications. In another case, domestic laws do not provide for any fixed term of office for the Head of the FIU or on which specific formal grounds the Head can be transferred or dismissed (laws make reference to the general provisions in place for "civil servants"). Another respondent highlights that during the time of appointment (which can be renewed only once) the Head of the FIU cannot be removed.

Responses to the Survey do not refer to any particular planned changes to the appointment/removal procedures. Nevertheless, in one case, it is reported that the possible future integration of the FIU into the Tax and Customs Administration may lead to reconsider the relevant procedures.

The responses concerning the authority responsible for the appointment/removal of the Head of the FIU draw a varied picture of different bodies and relevant procedures, also depending on the status/nature of the FIU.

The Head of the administrative and "hybrid" FIUs is generally appointed/removed directly by the Head of the organisation within which the FIU is located or by the government or other national competent authority (e.g. Ministry of Finance, the Attorney General, the King, etc.), subject to a proposal by the Head of the organisation within which the FIU is located or by other competent authorities.

In some cases the appointment of the Head of the FIU is subject to a hiring application procedure or a public call, followed by a selection procedure where the merit of candidates is assessed.

The Head of law enforcement/judicial FIUs is normally appointed by the Head of the Police, the Minister of Interior or by the Public Prosecutor's office.

As regards the duration of the office, the Head of the FIU is frequently appointed for a pre-determined period of time (in general 3-5 years), which is frequently renewable once. In a few cases the Head of FIU is appointed for an indefinite term.

The following table summarizes the competent body and the procedure for appointing the Head of the EU FIUs, based on the information gathered through the Survey.

APPOINTMENT/REMOVAL OF THE HEAD OF THE FIU			
Member State	Nature of the FIU	Competent body	Procedure
Austria	law enforcement	The Ministry of the Interior	When vacant, the position is opened for applications and the criteria to be met by the candidates are described in detail. After the closing timeline, the applications are reviewed and (with additional personal meetings) the candidates are evaluated and a ranking is made. After that the applications are passed to the personnel committee of the MOI and the proposal made in the course of the ranking is approved.
Belgium	administrative	The King	- cf. Law of 11 January 1993 on preventing use of the financial system for purposes of money laundering and terrorist financing, Article 22 - cf. Royal Decree of 11 June 1993 on the composition, organisation, functioning and independence of CTIF-CFI
Bulgaria	administrative	The Chairperson of SANS	The appointment and the removal of the Director of the FIU is carried out with a written order signed by the Chairperson of SANS.
Croatia	administrative	The Director of AMLO is a senior civil servant. Civil servants are assigned to the work post by the decision of a Minister.	The decision on the appointment of the Director of AMLO is made pursuant to Art. 127 §1 of the Civil Servants Act and the Rulebook on the Internal Order of the Ministry of Finance. The civil servant is assigned to the work post of the Director of AMLO. AMLTF Law does not itself provide any fixed term of office for the Director and any specific formal grounds for his transfer or dismissal. However, as the Director is a senior civil servant the terms for transfer or dismissal can be found in Art. 132 and following articles of the Civil Servants Act.
Cyprus	Hybrid	The Attorney General.	The Head of the FIU is appointed directly by the Attorney General, without the involvement of the executive.
Czech Republic	administrative	The Minister of Finance	A standard selection process is conducted according to the provisions of the Act on State Service
Denmark	Hybrid	The State Prosecutor for Serious Economic and International Crime	The appointment or removal is by decision of State Prosecutor for Serious Economic and International Crime
Estonia	law enforcement	The Director General of the Police and Border Guard Board.	The Director General of the Police and Border Guard Board shall appoint the head of the Financial Intelligence Unit on a proposal of the Deputy Director General in the Field of Intelligence Management and Investigation for five years.
Finland	law enforcement	The Head of the National Bureau of Investigation	In case the sitting HoF resigns, the position is declared open. Due to organizational changes and reasons, this has not happened for about ten years. Instead, the Head of the NBI has appointed the HoF several times.
France	administrative	The Ministry of Finances	The ministry of Finances by an order. The Head of the FIU is nominated for 3 years, renewable
Germany	law enforcement	The Head (president) of the Federal Criminal Police office.	There are no formal procedures, the head of the FIU is appointed by his qualification.

Greece	hybrid	The Supreme Judicial Council	The Head of the FIU (and his alternate) is appointed by the Supreme Judicial Council. Within 15 days the Council's decision is endorsed by the Minister of Justice. The Head of the FIU is appointed to serve on a full-time basis for three years, which can be renewed only once. During these three years the Head of the FIU cannot be removed.
Hungary	hybrid	The Head of NTCA	The Head of HFIU is appointed for an indefinite term by the Head of NTCA upon the proposal of the Deputy Head for Law Enforcement and Investigation Authorities of NTCA.
Ireland	law enforcement	The Commissioner of An Garda Siochana	The Head of the FIU is the Detective Chief Superintendent with responsibility for the Garda Bureau of Fraud Investigation. As such appointment/removal falls within the remit of the Commissioner of An Garda Siochana
Italy	administrative	The Directorate of the Bank of Italy.	The Director is appointed/removed by the Directorate of the Bank of Italy, on the basis of a proposal from the Governor of the Bank, among persons with fit and proper requirement (suitable integrity, experience and knowledge of the financial system). The appointment lasts five years and may be renewed only once. According to the Regulation, the Director can be removed only if he no longer meets the conditions required for the appointment or if he is responsible for serious misconduct.
Latvia	administrative	The Prosecutor General	The appointment procedure is described in Section 50, Parts 4 and 5 of the Latvian AML/CFT Law namely: "(4) The Head of the Control Service shall be appointed to office, for a four-year term, and dismissed from office by the Prosecutor-General. The removal procedure is described in Section 49(2) of the Office of the Prosecutor Law, namely: "(1) The Prosecutor General shall appoint the heads of State institutions supervised by the Office of the Prosecutor for the term provided for by law. The Prosecutor General may dismiss a head of an institution during his or her term of office only for committing a criminal offence, for intentional violation of law or negligence which is related to his or her professional activity and has caused significant consequences and for a shameful act which is incompatible with the status of a head.
Lithuania	law enforcement	The Minister of Interior	The head of Lithuania FIU is appointed for a term of 5 years and dismissed by the Minister of Interior of the Republic of Lithuania in accordance with the procedure laid down by the law on Civil Service.
Luxembourg	judicial	The Prosecutor of the Luxembourg District Court	All prosecutors of the CRF are independent magistrates, appointed by the executive (and formally nominated by the Grand Duke) to Public Prosecutor's office at the Luxembourg District Court. Once nominated, it is the Public Prosecutor who appoints the head of the FIU and its other magistrates. These appointments are unlimited in time and terminated at the discretionary decision of the concerned
Malta	administrative	The Prime Minister following consultation with the Minister for Finance.	The Chairman of the Board of Governors is the Head of the FIU. The Chairman and deputy Chairman of the Board are appointed from among the members of the Board by the Prime Minister following consultation with the Minister for Finance. The Chairman is appointed for a 3 year term and can be relieved of office by the Minister for Finance after consulting the body that nominated him for appointment. The Director which is responsible for carrying out all the functions of the FIAU, is recruited by the Board of Governors of the FIAU following a public call.

			The Director's tenure of office is determined by the Board of Governors in line with employment legislation currently in force.
The Netherlands	hybrid	The King of Kingdom of The Netherlands	The King of the Netherlands by Royal Decree on joint advise of the Minister of Security and Justice and the Minister of Finance
Poland	administrative	The Prime Minister	The head of the FIU - the General Inspector of Financial Information - is designated by the Minister of Finance and appointed by the Prime Minister. The opinion of the Minister of Finance is not required for the PM to dismiss the undersecretary
Portugal	law enforcement	Head of Judicial Police and Minister of Justice	The head of the FIU is appointed upon proposal by the Head of the Judicial Police to the Ministry of Justice from the board of high officials of the Judicial Police, based on his/her integrity, qualification and experience.
Romania	administrative	The Government of Romania	The Office is managed by a President appointed by the Government among Members of the Board. The Board is the debating and decisional structure, including one representative from the Ministry of Economy and Finance, Ministry of Justice, Ministry of Interior and Administrative Reform, General Prosecutor's Office by the High Court of Cassation and Justice, National Bank of Romania, Court of Accounts and from the Romanian Banks' Association, named in this position for a 5 year period, by Governmental Decision, subsequent to the proposal of the respective institutions
Slovak Republic	law enforcement	The Head of the National Criminal Agency	The Head of the FIU is appointed/removed by the order of the Head of the National Criminal Agency
Slovenia	administrative	Government of Republic of Slovenia	Appointment/removal of a Director is regulated by the Civil Servants Act. An appointment starts with a public call for a post. All applications are revised by a Special expert contest commission which gives an expert statement about candidates to State secretary on Ministry of Finance which proposes the appointment to the Government. Director is appointed by Government for a period of 5 years with the possibility of reappointment.
Spain	administrative	The Commission for the Prevention of Money Laundering and Monetary Offences	The Commission has the power to appoint and remove the Head of the FIU. Its decision is made at the proposal of the Secretariat of State for the Economy (President of the Commission), after consulting the Bank of Spain.
Sweden	law enforcement	The Head of National Operations Department (NOA) within the Swedish Police Authority.	The Head of the Financial Intelligence Unit is appointed after an application for employment by the Head of National Operations Department. The appointment shall last four years and may be renewed.
United Kingdom	law enforcement	The Director of the Economic Crime Command or the Director General of the NCA	Post would be advertised if needs to be filled, and competency-based assessment undertaken. Removal would be in line with NCA policies of retirement or resignation, or any discipline issues - the same goes for all UKFIU posts.

Table 6. Appointment/removal of the Head of the FIU

5.3 Decision making procedures

All respondent FIUs state that they are independent in decision-making processes related to their core functions of receipt, analysis and dissemination, as well as to the associated exercise of powers to obtain information and to exchanges with other FIUs.

Decision-making procedures are in almost all cases entirely self-contained within the FIU, without external interferences, and are centred on the Head of the FIU: he/she is the ultimate decision-making authority, as regards both operational and internal organization matters.

In some cases, especially in "bigger" FIUs, decisions can be delegated to specific internal structures, units or officers, which act in compliance with guidelines provided by the top level.

A special methodology for analysts is frequently established and implemented by providing instructions to be followed in working procedures, describing different phase actions of the analytical process and identifying duties and responsibilities.

A respondent has highlighted that the identification of strategic goals and priorities for the FIU, all decision-making processes regarding, for example, operational and strategic analysis, the postponement of transactions, the inspective planning, the relationship with domestic and foreign counterparts are developed within the FIU itself, without interference from third parties or from the organization where the FIU is embedded. The ultimate responsibility for the operations lies with the Director of the FIU.

Similarly, another respondent indicated that decision-making processes are carried out internally at the FIU, without any external interference. The Director is the one who has the ultimate word on the different topics, although most of the tasks related to international exchanges are delegated. As regards specifically analytical activities, the procedure usually consists of: preliminary examination (after which the decision could be opening a file for the specific case or rejecting it); after opening a file, this is assigned to an analyst, who carries out the analysis and the outcome is signed by the Director.

Based on responses to the Survey, FIUs do not envisage particular forthcoming changes to existing decision-making processes or to their internal organisation. One FIU has flagged that, to better cope with the increase in the volume of STRs, there are plans to improve automatic filters within the FIU.NET network to support the first level of analysis decision, thus simplifying and streamlining internal analysis procedures through faster screening and prioritisation. Another respondent has indicated that, in the context of the transposition of the fourth Directive, a review of its SARs regime and procedures will be undertaken with a view to improving effectiveness as well as the efficient use of resources.

5.4 Accountability

As already underlined, FIUs should be operationally independent and autonomous and, more particularly, should have the authority and the capacity to carry out their functions freely in order to fulfil their tasks properly and efficiently. At the same time, an enhanced status of independence and autonomy normally brings with it a need for making appropriate information available on the FIUs' activities, in a way that allows appropriate transparency and accountability of the FIU vis-à-vis different categories of external partners and stakeholders.

Responses to the survey show that, in fact, EU FIUs have developed a range of practices and mechanisms which, through different forms of information and communication, are aimed at ensuring that FIUs' activities and results are properly shared. This is in many cases also associated to the need to account for the use of the resources assigned to FIUs, particularly human and financial, vis-à-vis the objectives pursued and the relevant outcomes.

The means through which EU FIUs ensure appropriate accountability, as well the stakeholders to which the associated forms of information and communication are addressed, vary from Country to Country.

Responses show that in general, as regards the subjects to whom FIUs are accountable, the Head of the unit reports to the organization within which the FIU is located; reference in these cases is normally made to the competent Minister (or to a competent internal department). In other cases, the Head of the FIU is accountable to the Prime Minister or to the Government as a whole, to the Parliament or to Parliamentary Commissions in charge of overseeing the FIU. In other cases activities are reported to competent ad-hoc Committees in charge of overall coordination of national AML/CFT policies.

As regards FIUs that have a law enforcement status, these are normally set up within general police organisations, as said, and, therefore, their Heads is normally accountable to the Head of such organisations. In some cases, though, reference is made directly to the competent Minister (Home Affairs, Security and Justice). One respondent has indicated that it is accountable to the Prosecutor General and to the specially authorized prosecutors appointed by the Prosecutor General, who perform daily monitoring of the activities of the FIU, including on possible complaints regarding its activities.

For FIUs that have a "hybrid" nature, the Head is accountable to authorities that may vary from Country to Country: the Attorney General, the Prosecutor Office, a Special Parliamentary Committee, or, again, the Minister of Security and Justice.

The ways in which FIUs ensure proper accountability, and the tools used for this purpose, include various forms of reporting and communications. These range from the production of periodical reports illustrating the activities performed and the results achieved, to the compilation of ad-hoc statistics on volumes and types of disclosures and cases received, analysed and disseminated. Documents are also produced on emerging issues and methods in the field of combating money laundering and terrorist financing, as identified or elaborated in the FIU's activity. These reports and statistics are normally made available to competent authorities and are also published by the FIU.

One FIU mentioned that it currently does not produce an annual report but provides updates of its activities through the management chain of the authority within which it is located.

Other tools and procedures in support of FIUs' accountability consist in hearings in front of the Parliament or special Committees, as well as meetings between the Head of the FIU and members of the Government, of Ministers or other public authorities.

Although a wide range of different reports and statistics are produced and made available, the content and nature of the information, its structure and the media used appear to be in most cases pretty "traditional". Based on responses, for example, mass media and social media appear to be scarcely used, although FIUs' websites are normally structured as portals to access a broad range of information on FIUs' activities. Ad hoc forms of communication seem also rarely implemented, for

example in relation to particular successful operations or risk factors identified through the FIUs' activity. Forms of outreach, for example to the private sector or the general public, are also not mentioned in responses (besides targeted training initiatives).

ACCOUNTABILITY	
EU Member State or EEA State	**Whom is the Head of the FIU accountable to**
Austria	The head of unit in terms of administrative supervision.
Belgium	The Minister of Justice and the Minister of Finance
Bulgaria	The Chairperson of SANS
Croatia	The Minister of Finance.
Cyprus	The Head of the FIU may refer to the Attorney General on certain policy/strategic issues.
Czech Republic	The Minister of Finance and the Parliamentary Committee for the Control of FAU (only within the scope of decision-making processes)
Denmark	The State Prosecutor for Serious Economic and International Crime
Estonia	The head of Estonian Central Criminal Police
Finland	The Head of the NBI
France	The Ministry of Finances
Germany	The FIU is (due to the principle of legalism) operationally independent. The administrative and technical supervision is descried by the president of the Federal Criminal Police office.
Greece	The Special Committee on Institutions and Transparency of the Greek Parliament.
Hungary	The Deputy Head for Law Enforcement and Investigation Authorities of NTCA.
Ireland	The Commissioner of An Garda Siochana
Italy	The Parliament. The Financial Security Committee is also kept informed of UIF's activities.
Latvia	The Prosecutor General and the specially authorized prosecutors appointed by the Prosecutor General who perform daily monitoring of the activities of the FIU, including if there are any complaints regarding the FIU.
Lichtenstein	The Prime Minister
Lithuania	The Minister of Interior of the Republic of Lithuania.
Luxembourg	The Prosecutor of the Luxembourg District Court
Malta	The Minister of Finance, who, in turn, tables the Annual Report in the Parliament.
Netherlands	The Minister of Security and Justice in person.
Poland	The Prime Minister.
Portugal	The Head Of Judicial Police
Romania	The Government of Romania
Slovak Republic	The Head of the National Criminal Agency
Slovenia	The Minister of Finance
Spain	The Commission for the Prevention of Money Laundering and Monetary Offences
Sweden	The Head of the National Operations Department.
United Kingdom	The Deputy Director of the Economic Crime Command for day-to-day operations.

Table 7 - Accountability

6. Conclusions

The consolidated approach to FIUs' regulation in EU provisions, based on minimum or no harmonisation of domestic institutional and organizational features and a focus instead on the functions that FIUs have to perform and on the powers and information that should be available for that purpose, has resulted in a very diversified "landscape" of national solutions, whereby FIUs are all set up under different arrangements even within the three identified "models" of "administrative", "law enforcement" and "hybrid" units, and are organised along different institutional features.

In addition, the provisions in the fourth Directive about FIUs' necessary functions, information and powers lack details and, as a result, EU FIUs have different mandates and carry out different activities[31], contrary perhaps to the objectives pursued by the Directive for this part. This is particularly true for the analysis function, which varies considerably depending on the FIUs' nature and status and, for police-type FIUs, may even become absorbed into law enforcement activities. Ample differences exist also in the types and range of information available, equally due to the FIUs' status which determines powers and capabilities.

Together with domestic activities, these differences affect also the FIUs' capacity to cooperate and exchange information effectively among themselves.

For these reasons, the current paradigm underpinning the EU regulatory framework for FIUs, that is FIUs' nature and organizational features may vary provided that the same functions are exercised and sufficient information and powers are made available[32], may prove not to be correct and may need to be reconsidered. In fact, the extent of the flexibility allowed to Member States on the former aspects (nature and organizational features) influences the latter (functions, information and powers) and determines excessively divergent approaches with undesired effects also on FIU-to-FIU cooperation. Consideration should therefore be given to:

- setting minimum indications on domestic FIUs' features and organization, constraining in part the current excessive flexibility with a view to ensuring more convergence on functions and powers which is also conducive to better FIU-to-FIU cooperation[33];
- drafting more detailed provisions on the characteristics of FIUs' functions, notably as regards "analysis" as distinct from law enforcement activities, the underlying objectives and the information that FIUs should be able to receive or obtain to pursue them and to entertain effective cooperation.

The fourth Directive considerably expands FIUs' activities and related powers and at the same time, increases the complexity of such activities. This is particularly true in the area of FIU-to-FIU cooperation, where several innovations have been introduced. For example, EU FIUs are now required to make use of available domestic powers (that in turn have been expanded) to respond to foreign requests and to forward to interested foreign counterparts STRs/SARs that "concern another member State"[34]. As consistently indicated by respondents, these innovations bring about an increase in activities which are likely to put considerable strains on FIUs' resources. This goes together with a workload that is constantly increasing, particularly as regards the volumes of STRs/SARs received, the information exchanged between counterparts, and the demands associated with different forms of domestic cooperation.

Although responses to the Survey seem to indicate that available financial, human and technical resources are in general adequate to meet existing needs, concerns are also widely voiced by EU FIUs as to the FIUs' continued capacity to face expected developments in the absence of significant increases in available resources. In this context, faced with an expanded mandate and a higher level of complexity of their "core" functions associated with the receipt, analysis and dissemination of

[31] Depending, of course, on a number of national peculiarities concerning the structure of the AML/CFT system, the overall legal system, the institutional framework and the distribution of tasks and competence in the domestic context.
[32] This paradigm is explicitly recalled in article 3 of the Council Decision 2000/642/JHA: "Member States shall ensure that the performance of the functions of the FIUs under this Decision shall not be affected by their internal status, regardless of whether they are administrative, law enforcement or judicial authorities". The same principle is reiterated in the fourth Directive, specifically in relation to the FIUs' capacity to engage in cooperation activities (article 52).
[33] Making allowance for functions that are considered as ancillary and complementary to FIUs' core functions.
[34] See Chapter 6 on these aspects.

STRs/SARs, as well as with the related forms of domestic and international cooperation, FIUs (and Member States) should also reflect on few additional considerations.

- As seen, EU FIUs perform a number of tasks that are additional to their core functions. These tasks, despite the commonalities, are particularly diverse, as diverse are also the types and status of the EU FIUs. As a consequence, available resources, particularly human and financial, are distributed across all these functions, thus somehow reducing the portion that would be available for the exercise of core tasks. Anticipating the impact of the innovations brought about by the fourth Directive (and the increase of workload), it seems advisable that FIUs (and Member States) make efforts to recast their tasks with a view to concentrate resources on the effective performance of core activities as mandated by the Directive. As flagged by some respondents, this objective should be achieved also by improving the efficiency of working procedures and developing appropriate IT tools in their support.

- Ampler FIUs' operational independence and autonomy, as also required under the Directive (and international standards), is also conducive to achieving a higher level of effectiveness and ensuring that the broader spectrum of activities and the associated enhanced powers are exercised responsibly and to their fullest extent. In particular, FIUs should possess resources which, without necessarily having to be assigned through dedicated budgets, should be commensurate with the organizational and operational needs and determined outside of undue political considerations (particularly if relevant decisions on the funding of the FIU are taken by the bigger host institution, the competent ministry or the general government).

Together with a broader spectrum of activities and powers, and the associated responsibilities, FIUs' accountability should also be improved. More information and statistics need to be produced and made available by FIUs on their activities and the relevant outcomes. This set of information should be forwarded to partner authorities and to competent policy makers. It should also be disclosed to the private sector and to the public in general. While a number of good practices may already be in place in Member States, this is an area that is not covered specifically by the current mapping exercise; it is nonetheless recommended that appropriate consideration be given to introducing minimum common requirements at the EU level to enhance EU FIUs' accountability in a sufficiently uniform framework.

On this note, while article 44 of the Directive on general national AML/CFT statistics seems to provide an adequate initial framework, more detailed indications on data sets and communication procedures suitable for FIUs' accountability might be appropriate. Moreover, forms of communicating particular cooperation activities, for example those related to cross-border STRs and joint analysis, could be more adequately devised at EU level[35].

[35] See the explicit reference to "cross-border requests for information" in article 44.

CHAPTER 2

OPERATIONAL AUTONOMY AND INDEPENDENCE

1. Introduction

According to the Directive, in addition to being central national units, unique to each Member State, FIUs have to be set up and organized as **operationally independent** and **autonomous** units, for the purposes of carrying out their core functions of receiving, analyzing and disseminating STRs and other information related to money laundering, associated predicate offences and terrorist financing, exercising the powers conferred on them to achieve this aim and entertaining cooperation with FIUs of other countries.

The Directive provides for a few details on what the requirement of operational independence and autonomy entails: based on appropriate national laws and regulation, FIUs should have the authority and capacity to carry out their functions freely, including the autonomous decision to analyse, request and disseminate specific information (see article 32(3)).

From the provisions in article 32(3) and Recital 37[36] of the Directive, as well as from international standards[37], it can be inferred that independence and autonomy conditions should also apply to the organization and functioning of the FIU. In order for the FIU to operate independently and support its capacity to autonomously analyse, request and disseminate information, it has to be provided with adequate organizational autonomy and with sufficient resources to carry out these activities, as well as with the capacity to manage the resources assigned directly and independently in discharging its functions and pursuing its objectives[38]. Therefore, the requirement of operational independence and autonomy has two aspects:

[36] According to which "all Member States have, or should, set up operationally independent and autonomous FIUs to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing. An operationally independent and autonomous FIU should mean that the FIU has the authority and capacity to carry out its functions freely, including the autonomous decision to analyse, request and disseminate specific information".

[37] See particularly FATF Interpretive Note to Recommendation 29.

[38] Article 32(3) of the Directive should be recalled on this point: "Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks". On FIUs' resources, see Chapter 1.
More detailed standards on FIUs' organization are spelt out in FATF Interpretive Note to Recommendation 29, Section "E" (specifically dedicated to "Operational Independence"), which deals with matters concerning the relations with the host organization and with other domestic authorities, resources and staff: "An FIU may be established as part of an existing authority. When a FIU is located within the existing structure of another authority, the FIU's core functions should be distinct from those of the other authority. The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively. Countries should have in place processes to ensure that the staff of the FIU maintain high professional standards, including standards concerning confidentiality, and should be of high integrity and be appropriately skilled. The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information".

- capacity of the FIU to take autonomous decisions and responsibilities in performing its "core" functions;
- availability of sufficient resources and capacity to manage these resources and to organise itself independently to pursue its functions by taking autonomous decisions.

Based on the responses to the survey, EU FIUs generally consider themselves in line with the operational independence and autonomy requirements, specifically as regards their capacity to take decisions in discharging their core functions without influence from third parties. Further analysis, though, show that several constraints are in place. The following paragraphs, based on the information provided by respondents, are dedicated to an analysis of the FIUs' capacity to exercise their core functions[39] (par. 2.1) and powers (par. 2.2) under appropriate independence conditions, to engage in domestic and international cooperation independently (par. 2.3), to dispose of adequate resources and manage those resources autonomously (par. 2.4).

The focus of this Chapter will therefore be specifically on how FIUs' activities and powers are exercised, with a view to understanding whether appropriate autonomy and independence conditions apply. Separate Chapters will deal with the scope and characteristics of such activities and powers, with a view to determining whether, the independence conditions aside, FIUs have adequate capacities to receive and obtain information (Chapters 3 and 4), discharge their core functions (Chapter 5) and engage in international cooperation (Chapter 6).

2. Operational autonomy and independence in the exercise of FIUs' functions

2.1. Autonomy in the receipt of STRs/SARs

The FIUs' independence in receiving STRs/SARs may be translated into two main elements: a) the capacity of FIUs to obtain these disclosures directly, that is from the reporting entities themselves and without the interposition of any third party which receives the information before this reaches the FIU and, possibly, decides on its subsequent forwarding to the FIU; b) the capacity of FIUs to receive the disclosures exclusively, i.e. without these being submitted (in parallel) by reporting entities to other recipient agencies, which would contrast with the FIU's role as the unique central unit in charge of this function and of the associated evaluations and follow up[40].

2.1.1 Interposition of other bodies

As to the first point, the general rule is that FIUs receive STRs/SARs directly, that is without the interposition of other subjects and without any filter. No exceptions to this general fundamental rule are established, outside of cases, as allowed by the Directive and to the extent they are specifically provided for by domestic legislation, where some categories of obliged entities are authorised to file their disclosures to competent self-regulatory bodies. In fact, in accordance with article 34(1) of the Directive in relation to certain obliged professionals[41], Member States have the possibility to

[39] It has to be recalled here that the requirements of operational independence and autonomy only apply, based on article 32(3) of the Directive, to the "core" functions of FIUs and not also to the other tasks that FIUs may carry out based on domestic legislation and arrangements (see Chapter 2, par. 3).

[40] The fact that the FIU is the exclusive receiver of STRs/SARs filed by obliged entities derives from both the interpretation of the independence and autonomy requirement and from the direct application of article 33 of the Directive, which stipulates that, in fact, reporting entities should forward STRs/SARs to the FIU.
Of course, besides the reporting phase, nothing prevents STRs/SARs information being shared by the FIU with other domestic agencies, particularly trough dissemination, either spontaneous, following appropriate analysis, or on request, in cases provided for by national laws.

[41] These are: lawyers, auditors, external accountants, tax advisors, notaries, real estate agents.

designate an appropriate self-regulatory body as the authority to be informed in the first place, instead of the FIU.

These forms of indirect reporting, and their implementation in Member States, will be more specifically recalled and discussed in Chapter 3 when dealing with the information received by FIUs through STRs/SARs and the modalities and procedures supporting the receipt function. What is important to emphasize here is that the interposition of other bodies between the reporting entities and the FIU also impedes the FIUs' independence in receiving STRs/SARs, which requires that this should be directly and exclusively forwarded to the FIU. It is also for these reasons that the exception to direct reporting to the FIU is particularly limited and contained within particularly narrow boundaries: the body which receives the disclosures in the first place can neither retain this information nor apply some filters. Article 34 of the Directive, in fact, stipulates that the receiving organization is required to "forward the information to the FIU promptly and unfiltered", so that the FIU remains the central national agency gathering all STR information, thus retaining its independence and autonomy under this particular respect.

As will be more amply illustrated in Chapter 3, responses seem to show that only few Member States and FIUs have availed themselves of this option. In cases where indirect reporting mechanisms are allowed, these generally constitute an option for the obliged entities belonging to the relevant professional categories: they can opt for disclosing information via their self-regulatory organizations but remain free to send STRs/SARs directly to the FIU, if they so prefer. Moreover, as mandated by the Directive, the interposed self-regulatory organizations that are allowed to receive the disclosures in the first place are normally obliged to forward them to the FIU ("promptly") and are prevented from setting them aside, thus not informing the FIU about reported cases, or from even filtering out information included in the disclosures.

For example, a respondent informs that its national law expressly establishes that certain categories of professionals (i.e. notaries, labour consultants) shall send the report directly to the FIU or to their professional associations, which in turn shall transmit it without delay to the FIU. In this case, the professional association is merely a transmission channel, whose aim is to facilitate the reporting activities of the professionals. In line with the Directive, the professional associations have no discretion in its forwarding activity and cannot, for example, decide to archive the STR without sending it to the FIU.

It appears, however, that there are cases where the interposed self-regulatory organizations are entitled by national law to exercise some evaluation on the disclosures received and apply some filters on their content.

On this note, a respondent to the Survey has reported that, in its national system, lawyers are allowed to first send their STRs to the head of their self - regulating body; this, in turn, sends the disclosures to the FIU after evaluating if the conditions provided by the AML/CFT law are met. In particular, the self -regulating body has the power to verify that the limitations and safeguards applicable to the legal professions in reporting suspicions detected in their activities have been duly complied with.

To the extent that this evaluation entails an exercise of discretion, which can translate into STRs not being (entirely) forwarded to the FIU, this system may raise issues of misalignments with the requirements in the Directive on this point which, as said, also reflects on the FIU's independence in the receipt function which would be limited by the interposition.

Besides the interposition of self-regulatory organization in cases allowed by the Directive for certain categories of reporting professionals, responses do not refer to other instances where STRs/SARs are not reported directly to FIUs, which therefore seem to retain in all other cases full independence in their receipt functions.[42]

2.1.2 The FIU as the only recipient of STRs/SARs – Exclusive and multiple reporting

The second element defining FIUs' operational independence and autonomy in the receipt function, as said, pertains to their feature of being the unique recipient of STRs/SARs from reporting entities in the national context. Responses indicate that this is indeed the case for the vast majority of EU FIUs: they act as the exclusive national recipient of the disclosures filed in accordance with article 33 of the Directive.

Responses also show, however, that there are cases where, although the FIU receives the STRs/SARs from reporting entities, these are at the same time required to forward the same disclosures also to other domestic bodies[43]. In several cases, these additional recipients are fiscal authorities, which can therefore use the suspicious transaction reports for their activities aimed at detecting or pursuing, rather than money laundering, fiscal violations.

Multiple reporting to fiscal authorities

A respondent to the Survey has indicated that obliged entities are required to send STRs, at the same time, to the FIU and to the competent State Revenue Service/Office, in the event of particular indicators of suspicion regarding possible illegal activities in relation to tax violations. In this case, it looks like reporting entities are specifically required to assess the existence of tax-related suspicions and, for this subset of cases, forward disclosures to multiple recipients (the FIU and the fiscal agency)**.**

Another respondent has indicated that obliged entities are explicitly required to submit all disclosures, simultaneously and in the same format, to both the FIU and the national fiscal agency. In this situation, a comprehensive double reporting requirement seems to be in place, whereby all STRs/SARs, conceived for AML/CFT purposes, are transmitted by reporting entities to multiple recipients. It can be assumed that, as a consequence, all disclosures, while made subject to analysis by the FIU to identify possible money laundering or terrorist financing, are used in parallel to identify and pursue tax offences.

[42] It is interesting to note that other forms of indirect reporting were in place in some EU Countries in the past. This was notably the case of national systems where disclosures were filed by reporting entities (not limited to those belonging to certain professional categories) to a police body or a prosecutor, who would only afterwards forward the information to the FIU. These systems were even explicitly acknowledged and allowed by the previous third Directive (2005/60/EC), whose Recital 29 first clarified that "Suspicious transactions should be reported to the financial intelligence unit (FIU), which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing" and then concededthat "this should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIU, allowing them to conduct their business properly, including international cooperation with other FIUs". This derogation has been upheld by the fourth Directive.

[43] These situations are of course different from cases of direct access by other authorities to the STR information received and held by the FIU: see the discussion in par. 2.3 on this latter point. While in both instances other domestic agencies are in a position to obtain STR information directly, that is without the FIU's dissemination, this results is achieved differently, either through direct reporting from obliged entities (which impacts on the FIU's independent function of receiving and disseminating), or through direct ex-post access to the information already received (with consequences specifically on the FIU's dissemination function). In both instances, the independence and effectiveness of FIUs' activities are at stake.

In other instances, the disclosures are sent, besides the FIU, to law enforcement agencies or prosecutorial offices. In such cases, it appears that investigations or legal proceedings may be started on suspicious money laundering (or predicate offences) and terrorist financing cases, in addition to the analytical activities developed by the FIU on the same disclosures. These investigations or legal proceedings may be started and conducted, on the basis of the information provided in STRs/SARs, prior to, and possibly regardless of, the dissemination by the FIU, which is precisely intended to provide law enforcement and prosecutors with useful inputs for their activities based on the outcomes of the analysis.

Multiple reporting to police or prosecutors

A respondent clarifies that a copy of the STR/SAR is to be reported also to the law enforcement agency when the reporting entity is aware that there is a law enforcement interest. Similarly to what has been observed above for suspected physical violations, the double reporting seems applicable here to only some suspicious cases. Moreover, some precautions are provided to ensure that the FIU remains the direct recipient of the reporting flow in any case: the respondent informs that the failure to notify the FIU directly could be considered an offence and would not give a defense against any money laundering charges that may subsequently be brought subsequently.

In another instance, a respondent indicates that its national law provides for a dual reporting regime under which obliged entities, in all cases and regardless of any particular assessment, are required to send their disclosures not only to the FIU but also to the Attorney General.

Another case of multiple reporting is described by a respondent that indicate that, based on the federal organization of the Country and of the police authorities in charge of AML/CFT activities and investigations, disclosures are forwarded directly by obliged entities to the local law enforcement agencies (at the state level) and are also sent "in copy" to the FIU (at the federal level). This latter has then the role to provide support to local law enforcement actions. In this case, the reporting obligation has to be applied both at the federal and at the state level, sending the same disclosures to recipients additional to the central FIU.

Systems where dual or multiple reporting systems are in place, besides not being foreseen by the Directive (which, as said, assumes that the FIU should be the unique national recipient), raise several concerns. STRs/SARs information, collected for the purpose of allowing the analysis by the FIU on potential money laundering or terrorist financing cases, is used also for other purposes and by agencies other than the FIU, before and regardless of the FIU's dissemination. In parallel with the FIU's analysis, investigations may be started on the same facts and based on the same information, which certainly may bring peculiar challenges in terms of coordination of actions by different agencies and consistency in findings and results. These challenges, which are certainly more acute than those arising in systems where investigations are normally initiated following the FIU's dissemination and not upon direct receipt of STRs/SARs, can be further illustrated by the following points.

- Autonomy of the FIU in its receipt function (and other core functions). The rationale of centralizing all STRs/SARs disclosures, and the related information gathered through analysis, in the FIU is to allow this central unit to develop autonomous analysis under a "holistic" and comprehensive approach with the aim of then triggering possible follow up through investigations or prosecutions by other competent authorities. Differently from this approach adopted by the Directive, systems of multiple reporting allow to start parallel actions by the different agencies appraised, for different purposes under the respective

areas of competence. In cases where the disclosures are sent at the same time to the FIU and to police agencies or prosecutors, the distinction between analysis and investigations becomes blurred and the former would be made subject to the latter, with possible implications on FIUs' independence and quality analysis. This limits the independent operations of the FIU as its analysis may be conditioned, influenced by, or even absorbed into these parallel investigations or prosecutions. Direct upfront disclosure to multiple agencies may prevent the FIUs from adding value through analysis and subsequent dissemination. The dissemination function itself may also be in many cases overridden by the initial parallel disclosure.

- Coordination of functions. The centralized and exclusive reporting to the FIU, in the approach taken by the Directive, entails that the connection between the FIU's own and independent receipt and analytical functions and the actions subsequently undertaken by other competent authorities (based on the FIU's added value) lies in dissemination. It is through dissemination that the FIU shares the results of its analysis in support of ensuing actions. This happens, in the logic of the Directive and international standards, either through spontaneous dissemination or based on specific requests for information, which competent authorities can file to the FIU (as opposed to receiving initial STRs/SARs directly) precisely in order to gain insights into facts upon which they conduct investigations or prosecutions. Through dissemination the FIU and other interested agencies also ensure appropriate coordination of respective actions. Parallel direct disclosure to multiple agencies brings inherent coordination challenges, as each involved recipient will consider the information on its own and for its purposes[44].

- Purpose limitation. STRs/SARs, under the Directive, are triggered by suspicions of money laundering (or "associated predicate offences") and terrorist financing and are designed as information tools to trigger analyses by FIUs on the underlying cases. Any further use of these disclosures, through their direct transmission by reporting entities to other, non-FIU, agencies which would use the information for different purposes, does not appear in line with this approach. "Different purposes" include both the pursuance of violations other than money laundering or terrorist financing (such as stand-alone tax violations) and the conduction of investigations or prosecutions (as different from analysis)[45].

- Confidentiality and data protection issues. Multiple uses of STRs/SARs, or the pursuance of different purposes by multiple recipients of the same information, raise concerns also in terms of adequate confidentiality and integrity of these sensitive disclosures. The risk of tipping-off, explicitly prohibited by the Directive, is also increased under these circumstances.

While systems of multiple reporting appear to be rooted in national systems where the reporting obligation has been implemented by significantly departing from the centralized approach designed by the Directive, reinforced or clearer provisions at the EU level may be considered in order to ensure that, in each Country, the FIU should be the only recipient of STRs/SARs.

[44] Coordination issues may arise also in the context of cooperation between the agencies of different countries. In fact, in cases of cross-border phenomena, exchanges of information or other forms of cooperation (e.g. for the postponement of transactions or the seizure of funds) may be initiated by both the FIU and other domestic agencies that have received the same disclosures. Different cooperation channels and mechanisms may be activated simultaneously (e.g. at the FIU level and through MLA requests), with potential issues of coordination and conflicts.

[45] See the considerations in Chapter 6 on the meaning and scope of the "purpose limitation".

2.2. Autonomy in the analysis

While the main features of the analysis function, as highlighted through the survey, will be illustrated in Chapter 5, this paragraph is dedicated to the FIUs' capacity to perform this function under appropriate conditions of operational independence and autonomy. Based on responses, consideration will be given to the inception of analysis and the related triggering factors, the analytical process and tools, the final stage where the relevance of the case is assessed by the FIU for the appropriate follow up.

The survey shows that FIUs have a general positive perception of their capacity to perform their main functions autonomously. As regards analysis, in fact, all respondents have indicated that they have the capacity to perform this task by identifying and pursuing relevant cases taking autonomous decisions throughout the process.

2.2.1 Inception. Triggers and priorities

Responses indicate that FIUs decide autonomously when an analysis should be started. On this aspect, however, account needs to be taken of existing forms of influence on FIUs' determinations to conduct analysis, which can impact on the independence condition, exercised by external parties, notably by the organization where the FIU is located or police agencies or prosecutors in the context of law enforcement activities. When investigative or prosecutorial activities are underway on the same case, the FIU could be required to start and develop targeted analyses in support of such activities. Decisions in this respect may be driven by competent law enforcement bodies as well as from staff within the organization where the FIU is located, with a reduced room for independence for the latter (this point will be further illustrated in paragraph … on links between FIUs and external parties).

Of course, the decision to initiate analytical activities, while generally taken autonomously by the FIUs, is not adopted on arbitrary bases. In fact, FIUs' analysis is triggered by a number of factors, first and foremost the receipt of STRs/SARs. Information collected elsewhere can also trigger analysis, to the extent that this information is indicative of potential money laundering or terrorist financing cases and that the FIU has the legal capacity to act upon it.

A respondent to the Survey specifies that financial analysis is exercised not only on STRs but also on unreported suspicious transactions of which the FIU becomes aware on the basis of, i.a., information contained in its databases, obtained through onsite inspections or sent by law enforcement agencies, supervisory authorities, self-regulatory bodies, foreign FIUs.

Similarly, another FIU indicates that it acts upon suspicious transaction reports filed by obliged entities, but also on other information concerning possible money laundering or terrorist financing activities transmitted by public or private agencies or foreign FIUs or otherwise learnt through mass media or any other source.

An important consideration for FIUs when initiating analysis is to establish the level of priority of the cases that should be considered. This is essential especially when there is a sheer volume of information to process (due to, for example, the number of incoming STRs or other disclosures) and resources have to be deployed appropriately, distributing them among multiple cases which cannot be all developed in parallel. This is also important because, under the Directive, the analytical function (and the dissemination as well) has now an element of "selectivity" which requires FIUs to consider all available information but, at the same time, to focus on relevant cases for analysis and

ensuing investigations by competent bodies on actual money laundering or terrorist financing cases[46].

Appropriate independence and autonomy should be exercised by FIUs in deciding about conflicting priorities taking account exclusively of the relative importance of the cases under consideration. Decisions should of course be taken in light of any possible input provided by other agencies (for example, on ongoing investigations) but without undue interferences. This aspect is highlighted by only few respondents, which confirm that they are able to decide autonomously on priorities for their analyses[47].

These respondents emphasize that they perform analysis based on their own procedures, judgment and decisions and that priorities are also established in autonomy, of course taking full account of any relevant information and valuing the dialogue with other relevant authorities.

The lack of sufficient resources to cope with increasing workloads, besides forcing FIUs to sharpen their capacity to identify and solve conflicting priorities, may impact on FIUs' operational independence and, at the same time, on their operational effectiveness. In fact, respondents highlight the challenges they face due to the higher volumes of STRs/SARs, which is putting available resources under increasing strain. Human resources and dedicated IT tools would need to be adjusted and upgraded to keep up with FIUs' increasing workload. Difficulties may be more significant for FIUs that are not provided with their own budget or with adequate financial resources. As respondent FIUs also stress, an increase in resources should be complemented by improvements in working methods and procedures, so as to enhance efficiency.

2.2.2. The analytical process

After the inception phase, FIUs should also carry out the analytical process in an independent manner, determining the most appropriate means and resources to deploy, relying on their own tools and powers and deciding on appropriate steps and timeframe. This process should be driven by FIU's considerations about the features of the cases under analysis, their complexity and level of priority, the objective to produce a useful outcome based on actionable intelligence for subsequent investigations or prosecutions. In this context, for example, FIUs should be able to decide freely which information should be obtained and whether other domestic authorities should be approached with requests or foreign FIUs contacted for sharing information on relevant cross-border elements.

Responses to the Survey seem to indicate that EU FIUs are generally capable of managing and shaping the analytical process taking autonomous decisions. References are also made to structured procedures implemented to ensure that analyses are carried out in an efficient and consistent manner, also by making use of ad-hoc IT tools. Obviously, information powers and other tools in support of the analysis can be actioned by FIUs to the extent and within the limits and conditions established under domestic laws (see Chapters 4 and 5 on FIU's information and powers).

A respondent indicates that, in the course of analysis, it conducts checks in own databases, other databases of the parent organization as well as other registers accessible to the FIU. Depending on the case, additional information can be collected, for example to establish the economic

[46] See article 32(8)(a) of the Directive. For more details on this matter concerning the feature of the analysis and dissemination functions see Chapter 5.

[47] Concerns remain, though on the actual capacity to establish priorities autonomously and without interference for FIUs that are embedded in bigger organizations and are subject to hierarchical links with respect to such organizations or external parties (see the following paragraph 5).

background and the transaction patterns. In general, the FIU is entitled to collect any data on natural or legal persons which is deemed necessary for the prosecution of money laundering or terrorist financing. What kind of information will be collected is decided individually following the assessment of the facts of case. In cases involving a foreign country, additional inquiries can be directed to the country affected; if required, cross-border meetings can be organised at short notice.

Other FIUs also flag that the analytical procedure is carried out by the FIU without external interference. In particular, disclosures are analyzed and assessed by a case officer who has to decide if the case can be disseminated or the level and type of analysis that should be performed, for example by obtaining more information from obliged entities, from foreign FIUs or from other agencies.

An FIU mentions that, while currently almost all STRs have to be manually considered and assigned to analysts for appropriate treatment, the introduction of a new IT system will perform some basic inquiries promptly, allowing to select cases that, in light of their features and low complexity, can be brought to conclusion immediately.

Some respondents indicate that external staff from law enforcement agencies can be associated to the analytical activities of the FIU. This can be the case when complex cases have to be dealt with that require additional skills or a multidisciplinary approach; or when there are connections with investigations or a need to use STRs/SARs material also in the context of investigations. This approach has been reported by FIUs that have a law enforcement status and are embedded in police organizations. Safeguards are applied in these cases to make sure that the "seconded" staff works exclusively for the FIU on the particular cases assigned and is bound by appropriate confidentiality duties.

A respondent explains that in very complex cases, the FIU receives technical and analytical support by an officer from the bigger police organization where the FIU is located. This officer, in discharging such duties, becomes a functional member of the FIU and, as such, is subject to the FIU's obligation of secrecy. In less complicated cases, operational analysis is conducted by FIU's case officers in charge.

Another FIU has indicated that, while it only performs intelligence analysis and it is for law enforcement agencies to pursue evidence and analysis in order to take a case to court, the FIU also allows for STRs/SARs to be analysed by accredited staff from law enforcement agencies. These agencies are required to notify the FIU where STRs/SARs are to be used in a prosecution and, based on agreements with the FIU, to give regular feedback on the use of SARs.

The involvement of external staff into FIUs' analysis provides opportunities to exploit synergies with other agencies, leverage on a broader set of skills in complex cases, maximise the use of resources and possibly compensate for lack of FIUs' staff especially in cases of increasing workload. At the same time, however, the participation of outside officials into the conduction of core functions of the FIU, within its organization and through its procedures, may raise potential issues.

In the absence of adequate safeguards and controls, the access by external staff may cause STR/SAR information to be unduly shared or circulated and used for purposes other than analysis by the FIU (for example, in ensuing or parallel investigations where the same staff may be involved). The continuity in the use of FIUs' resources may also be affected, due to turnover of analysts. Potential impacts on the operational independence of the FIU should also not be underestimated; systematic or excessive dependence on external staff may be an indicator of

insufficient capacity of the FIU's to discharge its core functions. Also, relying on, and employing, external resources might affect the FIU's capacity to manage its tasks autonomously and under appropriate confidentiality requirements. Seconded analysts, whilst not fully integrated into the FIU's organization, may remain subject to direction by the organization of origin. This risk may be heightened for FIUs that are embedded as an integral part of the police agency that seconds the analysts.

These concerns can be mitigated through appropriate measures. As the responses on this point also seem to suggest, the use of external resources within the FIU should go together with the setting of appropriate control and clearance procedures, to make sure that access to sensible information is commensurate to the analysis needs and is always adequately monitored. At the same time, external staff employed within the FIU should respond to the FIU's hierarchy for any matter concerning the analytical work, rather than to officials from the agency of origin.

2.2.3. Conclusion of the analysis

Autonomous decisions should also be taken by FIUs concerning the conclusion of the analytical process, particularly as regards the need to forward the analyzed cases to competent law enforcement agencies or prosecutors, accompanied by the intelligence gathered, for the appropriate follow up, or the possibility to close the procedure and set aside those cases that, in light of the analysis, turn out not to be founded or suspicious.

The need for FIUs to take a selective approach on cases and on information has to be recalled in this perspective[48]. Decisions have to be taken, in an independent manner, on the identification of relevant cases which deserve an investigative follow-up, the assignment of motivated priorities to such cases, the compilation of the intelligence developed through analysis capable to support ensuing investigations, the selection of the accompanying information.

This process is described by a respondent that points out that, once the FIU has collected the necessary information, it assesses the facts of the particular case and decides whether further investigations by other offices (or the FIU itself) are necessary. The FIU's decision on whether to confirm the suspicion of money laundering depends on various factors; in particular, on whether information indicates that the funds may originate from criminal activities or that any layering activities have been performed. In this case, formal investigative proceedings are initiated. If there is no further information suggesting any punishable offence, the FIU closes the file.

Responses to the Survey seem to confirm that EU FIUs are generally in a position to decide autonomously when the analytical process is complete, all necessary intelligence has been developed and the case is ripe for a decision on the required follow-up. In any event, the FIUs' capacity to determine freely the conclusion of the analysis has to be considered together with possible conditions or constraints applicable in the subsequent dissemination, particularly as regards the scope of the information forwarded and the range of recipient agencies. The independence requirements in the dissemination phase are dealt with in the following paragraph.

2.3. Autonomy in the dissemination

The FIU's capacity "to carry out its functions freely" includes, in accordance with article 32(3) of the Directive, "the ability to take autonomous decisions to analyse, request and disseminate specific information" to competent authorities. The same article goes on by saying that the dissemination by

[48] See more on this in Chapter 5.

the FIU concerns "the results of its analysis" (not all the information that has been received or processed) and needs to be done "where there are grounds to suspect money laundering, associated predicate offences or terrorist financing", based on the analysis performed. Decisions on dissemination, including when and what to disseminate, therefore, have to be taken by FIUs freely, with no interference from third parties.

The FIUs' capacity to decide independently on whether information should be "spontaneously" disseminated after the analysis should not prevent FIUs from duly responding to requests for information by competent domestic authorities under the different regime of the dissemination "on request" (which is not dependent on the analysis and on its outcomes). In this regard, the Directive requires that FIUs should "be able to respond to requests for information by competent authorities in their respective Member States" (article 32(4)). Precisely with a view to safeguarding the FIU's independent operations, this provision also establishes limitations and conditions that ensure that the FIU, while providing cooperation and information to competent authorities, remains autonomous in performing its functions. In fact, the third parties' requests for dissemination should be "motivated by concerns relating to money laundering, associated predicate offences or terrorist financing"; secondly, and more importantly, "the decision on conducting the analysis or dissemination of information shall remain with the FIU"[49].

The Report will focus specifically on spontaneous dissemination. In light of the provisions of the Directive, the requirement of FIUs' operational independence with regard to the exercise of the dissemination has multiple dimensions and needs to be considered under different angles:

- the decision on whether or not a case should be disseminated (outside of cases of dissemination on request provided for by national law in accordance with article 32(4));
- the decision on the timing of dissemination;
- the decision on the information that should be forwarded.

These aspects will be discussed in the following paragraphs (and in Chapter 5) in light of the responses to the Survey and to the limitations and shortcomings that seem to emerge. Other aspects will also be considered, as they are touched on by respondent FIUs, such as the identification of competent authorities as recipients of the dissemination and the indication by FIUs of the possible follow up for the disseminated cases.

Active dissemination vs. passive access to FIUs' databases

It is important to underscore that the dissemination function is based on an active role which should be played by the FIU: this has the responsibility to identify, through analysis, cases and information that need to be followed up in ensuing investigations or prosecutions and forward these cases and information to competent national agencies. Therefore, it is the FIU which actively "pushes" information on, based on its own initiative and decision and ensuring that the results of the analyses are properly highlighted and valued, also through adequate selection.

For these reasons, STR/SAR information should not be merely and passively made available for access by other agencies, upon the initiative of the latter and based on their own volition, through queries of the latter into the FIU's STR/SAR databases. Also, aside from cases of dissemination "on request" (see Chapter 5, paragraph 6), it is always the FIU that should be in control of dissemination activities (particularly as regards the "when" and the "what") and information should not be "pulled" from its databases by other domestic agencies.

[49] Additional conditions and limitations to FIUs' dissemination on request are set out in article 32(5).

Although responses to the Survey do not highlight particular issues on this point (but see the examples and practices recalled in Chapter 8, par. 3.4, under the particular angle of the confidentiality and security regime), evidence from FATF Mutual Evaluations show that, in the case of a Country which is an EU Member State the dissemination of STR information takes place primarily by passively allowing competent law enforcement agencies to access the FIU's database, rather than proactively forwarding relevant information:

"The analysis of UTRs consists mainly of matching the UTR information with other information the FIU has access to. In this case the UTR is classified as an STR and loaded into the STR database, which can be accessed by Law Enforcement authorities for criminal investigations concerning any crime, not only ML/FT. This task represents the most common way in which in practice the FIU is disseminating the information"[50].

In these cases where STR information are deposited in a "cloud" held by the FIU which can be accessed by competent law enforcement agencies, rather than being actively forwarded, it is not only the FIU's independence which is constrained in carrying out the dissemination function; more broadly, it appears that the dissemination function itself is not properly conducted in conformity with what is required by the Directive. The EU provisions, in fact, in line with FATF standards, assume that the FIU plays an active role in forwarding relevant information following its own analysis and based on its own decision and evaluations; in addition, the dissemination concerns "the results of the analysis", not the STR information per se, and as such has a necessary element of selection which the FIU should fulfil by filtering relevant cases.

The reasons for this peculiar configuration of the "dissemination" function, and the deviation from the approach underlying the Directive, seem rooted in the way in which the EU provisions have been transposed into domestic laws. However, consideration may be given to more explicitly clarify at the EU level that, aside from cases of dissemination upon request (as regulated in the Directive as not being a compulsory duty for the FIUs and derogated in a number of circumstances[51]), the FIU should be responsible for proactively (and selectively) forwarding information to competent recipient and that dissemination cannot be based on passive access to STR databases.

2.3.1 Independent decision to disseminate

Many respondents confirm that they take independent decisions on the outcome of their analyses and, accordingly, on whether the analysed cases should be disseminated, as they are indicative of money laundering or terrorist financing activities, or closed and set aside, as they turn out to be unfounded.

Similarly to what has been mentioned earlier for the analysis function, it is important to underscore that, while the FIUs' independence in the spontaneous dissemination stage entails that relevant decisions have to be taken by the FIUs freely and without interference, these decisions are certainly not arbitrary. In fact, they strictly depend on technical considerations based on the relevance of the case for the identification of money laundering or terrorist financing activities.

[50] The FATF Mutual Evaluation Report recalls that, "In addition to this modality, there are also other ways in which the information is pro-actively disseminated to law enforcement agencies".
[51] See article 32(4)(5) of the Directive.

Another important aspect to clarify is that, in accordance with the "FIU" definition, where dissemination is identified as one the "core" functions, there should be an outright obligation for FIUs to disseminate information in all cases where, based on the analysis, there are reasons to believe that money laundering or terrorist financing may have occurred. The independence requirement, in fact, lies in the FIU's capacity to determine whether the analysed cases are potentially linked to money laundering or terrorist financing and does not imply that, when it turns out that this is the case, the FIU can decide not to inform competent authorities for the necessary investigations or prosecutions.

Several responses describe how FIUs take independent decisions on whether or not to disseminate and how, in cases where dissemination is decided, this is based on the positive outcome of the analysis.

A respondent underlines that any interference within the FIU`s discretion to forward analytical reports to competent law enforcement authorities would be a breach of the FIU Act (and has never happened) and that, at the same time, the FIU is obliged by law to forward its reports whenever it deems the requirement of a ML/TF or predicate offence suspicion to be met.

Another respondent points out that STRs are transmitted, together with a technical report and relevant information, after the operational analyses and that spontaneous dissemination is done exclusively in accordance with the law and based on the FIU's own decision, whenever the analysis is complete.

Several other respondents confirm that decisions on dissemination are taken freely by the FIU based on the results of their analysis. The following are examples of the feedback received on this point.

- After the analysis, a decision is taken on whether to open a new (own) investigation or to disseminate the information to other domestic (or foreign) counterparts; the file can be closed under the FIU's own responsibility, in cases where the suspicions of the reporting entity is not confirmed by the intelligence gathered.
- Dissemination to competent law enforcement authorities is performed, pursuant to legislative provisions, when facts resulting from disclosures indicate that a criminal offence has been committed, or they may hamper or substantially impede the seizure of proceeds of crime or if the information relates to an on-going criminal proceeding and such information could be considered as important for this proceeding.

2.3.2. Timing of dissemination

Independent decisions have to be taken by FIUs also on the timing of dissemination, which depends on when the analysis is considered complete and on the "readiness" of the case. Should other parties be able to "pull" information from the FIU before the analysis is complete and dissemination is spontaneously performed, this would amount to a limitation of the FIU's "ability to take autonomous decisions to disseminate", contrary to article 32(4) of the Directive.

All responses to the Survey that touch on this aspect confirm that FIUs perform the dissemination after the analysis and when they consider that the case is ripe for appropriate follow up in light of the information gathered and the outcome of the analysis itself[52].

For example, a respondent explicitly mentions that it proceeds to dissemination "whenever the analysis is complete" and that this decision is entirely dependent on the FIU also for what concerns the timing.

2.3.3. Recipient competent authorities

In several cases, FIUs also take determinations on which competent authority should be the recipient of each particular dissemination, depending on the nature and the expected follow-up of the underlying cases. Responses seem to indicate that most often the recipient of dissemination is identified by the FIU among law enforcement agencies or prosecutors, also taking account of the possible existence of investigations or legal proceedings that are already ongoing.

In other instances, the FIU is obliged to disseminate cases and information to agencies that are specifically designated by the law, so that they do not have any discretion in this respect. In such cases, the FIU may not be allowed to forward information to agencies other than those designated by the law, regardless of the nature of the case, of the outcome of the analysis and also of possible existing investigations or prosecutions carried out by other agencies or prosecutors.

Several respondents to the Survey indicate that they forward the information to "competent law enforcement agencies", identified by the FIUs themselves based on the nature of the case and on the distribution of competences among different police bodies.

Some FIUs can also inform competent prosecutors, also identified based on particular circumstances of the case, when for example there are reasons to believe that a prosecution or a legal proceeding should be started or is already underway.

On the other hand, a respondent has pointed out that it disseminates STRs, together with a technical report and relevant information, to specific competent law enforcement agencies identified by the law which, in turn, may appraise competent police units or prosecutors.

Possible restrictions to the FIU's capacity to identify the recipient authorities, as those that, based on the nature of the case and the outcomes of the analysis, are in the best position to effectively pursue the necessary investigations or prosecutions, may result in limitations to both the effectiveness of the dissemination function[53] and the FIU's independence for this particular aspect of the dissemination function.

Whilst dissemination is by its nature aimed at triggering, or otherwise assisting, investigations or prosecutions on cases of money laundering, predicate offences or terrorist offences by competent police agencies or prosecutors, some respondents indicate that they can disseminate information also to other authorities, for additional, different purposes.

[52] See, however, the consideration in paragraph 2.3, on cases of direct access by law enforcement agencies to the FIU STR database. Together with the entire dissemination function, also the decision on its timing is taken out of the FIU in such cases.

[53] This may be the case especially when the law sets out a narrow scope of competent authorities as recipients of the FIU's disseminations.

For example, an FIU has recalled that, in addition to the ordinary dissemination to competent law enforcement agencies to pursue criminal cases of money laundering or terrorist financing, when supervisory action could be affected by a certain case it also informs the financial market supervisor. Similarly, another respondent underscores that it can disseminate cases and information broadly, to judicial and police bodies, Customs, tax administration, social administrations, regulators, intelligence services.

2.3.4. Disseminated information

As recalled, the requirement of independent dissemination has also another important dimension: the FIU should be able to establish, in light of the cases and the related analysis, the most appropriate set of information that should be included in the dissemination "package" to properly illustrate the intelligence produced and support the ensuing investigations.

The need to ensure this capacity to select relevant information that should accompany the dissemination is explicitly foreseen by the Directive under two different and complementary aspects. Firstly, in describing the core function of dissemination, article 32(3), third sentence, specifies that the FIU is required to forward "the results of its analyses and any additional relevant information", that is not all that has been received by the FIU through the initial disclosures or obtained in the course of the analysis. Secondly, in defining the requirement of operational independence and autonomy for the dissemination, the same article 32(3), first sentence, explicitly mentions that this entails the ability for FIUs to forward "specific information", that is not generally everything that has been processed on each particular case through receipt and analysis.

Therefore, FIUs' are not expected to forward all the information they receive or obtain. FIUs should exercise their independent judgment in selecting relevant information to disseminate, having regard to the outcome of the analysis and to the need to be "specific" in this regard, thus facilitating the ensuing investigations or prosecutions. As a consequence, possible situations where FIUs may be required to forward all the information they receive or process through dissemination, or are otherwise prevented from selecting intelligence elements gathered by focusing specifically (to quote the Directive) on the "results of the analysis" and on what they have reason to believe can assist competent authorities, should be considered for potential undue limitations to both the correct exercise of the dissemination function (in light of its description in article 32) and the FIU's operational independence in this particular respect.

Responses seem to indicate that the disseminated information normally includes the disclosures received and the relevant intelligence gathered through the analysis. At the same time, FIUs generally have the capacity to select the information to forward to competent authorities, with a view to ensuring that this includes useful intelligence for the necessary follow-up.

Responses to the Survey indicate that FIUs are generally under no specific obligations as to the set or types of information that should be included in the dissemination. For example, while STRs are normally forwarded to law enforcement agencies when they relate to well-founded cases, there is normally no obligation to transmit the disclosures in all cases.

It appears therefore that FIUs can exercise considerable discretion in determining the information that accompanies the dissemination, taking account of the nature of the cases involved and of the results of the analysis. FIUs disseminate the results of their analysis and the set of information, received or gathered through analysis, which is apt to illustrate such results and provide potential leads to ensuing investigations.

Other responses highlight that some FIUs are obliged by law to disseminate all received STRs/SARs, with no possibility to set aside those disclosures which, based on the FIUs' analysis, do not appear to be founded or, otherwise, do not contain strong indications of money laundering or terrorist financing activities. As indicated by these respondents, the rationale of this approach to dissemination is based on the consideration that recipient law enforcement agencies should anyway be appraised of cases reported as suspicious, as they can be in a position to extract further intelligence, beyond previous analysis by the FIU, taking account of additional police information, either available at the time of the dissemination or at a later stage.

A respondent, in particular, indicates that all information about STR/SAR are either actively disseminated (when the analysis gives a positive outcome) or in any event made available to competent law enforcement agencies (also for cases that are not deemed relevant). At the same time, however, while all STRs have to be shared, the FIU retains the capacity to accompany them with the information which is relevant to each particular case; an ad-hoc "technical report" is prepared for this purpose and always accompanies dissemination to illustrate the results of the analysis.

While in these cases the "selection" element may be less developed or pronounced (and the FIUs' independence consequently limited), with a possible lower level of filtering by the FIU on cases that are forwarded for investigative follow-up[54], the same respondent emphasizes that dissemination is accompanied by indications on the relevance of each case, also setting out "ratings" in terms of their potential connections with criminal activities. This is intended to allow appropriate prioritization and efficient allocation of resources by competent law enforcement agencies that receive the information (see also the following paragraph).

In some cases, the FIU is required to remove certain sensitive information from the dissemination package, notably that regarding the reporting entities and their employees, with a view to limit the exposure of reporting parties and not to discourage the disclosure. This information can be supplied to law enforcement agencies only when needed for legal proceedings and under certain conditions.

For example, an FIU points out that it is prevented from forwarding information on the reporting entity's employee who first supplied the information, except for instances where there are reasons to suspect that the reporting entity or its employee have committed the money laundering or terrorist financing offence, or if the information is necessary to establish the offence in the criminal procedure and the said information is required by the competent court in writing.

2.3.5. Indications on priorities and possible follow-up

An important element of the FIUs' capacity to perform dissemination in an independent manner by exercising their autonomous judgment, at the same time ensuring the appropriate selection of cases in light of the analysis, is the ability to assign priorities to disseminated cases, thus valuing the outcomes of the analysis and allowing recipient authorities to focus on most relevant cases of potential money laundering or terrorist financing.

On this note, a respondent emphasizes that the analysis it performs, articulated in multiple successive levels, focuses specifically on assigning "ratings" to the cases examined, based on their potential relevance for the identification of money laundering or terrorist financing. Following the

[54] The impact of this "universal" approach to dissemination may be particularly significant, especially on the overall capacity to identify priorities and to allow to deploy resources accordingly, in situations where the FIU receives a sheer amount of disclosures.

dissemination, competent law enforcement agencies therefore receive the cases categorized according to the rating assigned by the FIU and enriched by the intelligence gathered during the first and second level analysis.

Through dissemination, FIUs can in some cases also provide indications to the recipient law enforcement agencies on the most appropriate follow up for the disseminated cases, taking account of the elements highlighted through the analysis. The capacity to provide such indications, though not binding on the recipient law enforcement agencies or prosecutors, reinforces the FIU's status of independence in coming to autonomous conclusions in light of its analysis.

For example, one FIU emphasizes that it can disseminate the results of its analysis for different purposes and to different recipient: for conducting a deeper specialized analysis for intelligence purposes (recipient authorities are in these cases tax agencies, custom authorities, anti-terrorism or anti-corruption unit); for investigation purposes (disseminations are sent to, i.a., national police organisations or to the competent prosecutor's office).

2.3.6. Procedure for dissemination

The transmission of information through dissemination should normally be carried out by means of dedicated channels, so as to ensure the appropriate confidentiality and security. Dedicated IT tools could be set up for this purpose, especially in cases where the FIU normally forwards all its information to the same agencies.

For example, a respondent has indicated that a dedicated web-based "portal" has been set up to forward disseminated information to recipient police bodies in a confidential manner (these bodies are designated by the law as the unique recipient of the FIU's disseminations). Through this portal, STRs and related technical reports are forwarded to the two Law Enforcement Counterparts in real time.

On the same point, other respondents (in other sections of the Survey), emphasize the need to increase the use, and improve the quality, of IT tools in support of data analysis and the overall intelligence cycle, with potential spill-overs on effective dissemination too.

2.4. Autonomy in receiving or accessing threshold-based disclosures

The majority of FIUs have indicated that they receive directly threshold-based disclosures, as required by the law, or access such disclosures without depending on third parties' discretional authorization, in addition to STRs/SARs. On this regard, it is worth noting that some respondents highlight that they don't receive such type of disclosures.

Differently from STRs/SARs which are triggered by the detection of suspicions (regardless of the type of the underlying transaction or activity and of its monetary value), these disclosures become due for all transactions that meet specified objective features and reach or exceed a quantitative threshold. Most common types of such objectives disclosures are related to transactions performed with banks (deposits or withdrawals of cash) or other obliged entities (for example, purchase or redemption of fiches in casinos) and the physical transportation of cash or bearer instruments to or from other countries (in accordance with EU Regulation 1889/2005).

The EU FIUs' capacity to receive threshold-based disclosures, or to have access to the information reported, will be examined and discussed in Chapter 3, paragraph 3, specifically with regard to the nature and content of such disclosures and the reporting procedures and timeframes.

In most cases, threshold based disclosures provided for by domestic legislations are received directly by the FIU. In these instances, as confirmed by respondents, the FIUs can certainly use the information in such disclosures for their own analytical purposes in full autonomy, that is based on their own decision and with no need to obtain access through (or authorised by) third parties.

In other cases, threshold-based disclosures are forwarded by obliged entities to other competent recipient authorities. This typically happens for the declarations concerning the physical cross-border transportation of cash and bearer instruments, as specifically foreseen by the EU Regulation 1889/2005.

While FIUs that receive disclosures directly have of course no difficulties in using their content any time it is needed, it is less clear from responses if the same level of autonomous use is available to FIUs that have to gain access to objective disclosures received and held by third parties. Importantly, responses do not expressly mention the existence of undue restrictions to the FIUs' access in such instances, even though no feedback is available on possible conditions or limitations in this respect (deriving, for example, from discretion exercised by the Agency holding the information, data protection issues or timeliness problem).

2.5 Autonomy and operational independence in FIUs' powers

2.5.1 Autonomous access to external sources of information

FIUs should have the capacity to have access to the "financial", "administrative" and "law enforcement" information that they require "to fulfil their tasks properly" (article 32(4) of the Directive). The range and types of information falling under these general categories that are available to EU FIUs will be explored and discussed in Chapter 3, paragraphs 4 to 9, with regard to specific databases required by the Directive (notably, on bank accounts and on beneficial owners) and to other sources identified at national level. This paragraph briefly deals with the FIUs' capacity to access necessary information under appropriate independent conditions.

FIUs seem to confirm that they do have access to external sources of information, including data held by other authorities, without depending on third parties discretional authorization, including law enforcement data. The information provided through the Survey show, however, that some conditions may apply limiting the FIUs' capacity to obtain information needed for their activities in an independent manner; forms of discretional authorization by third parties are also referenced.

For instance, a FIU has indicated that if there are grounds to suspect ML/FT it may require from state authorities the data, information and documentation needed for detecting and proving ML/FT, also through direct electronic access to certain data and information.

Another FIU ha flagged that it has an independent on-line access to a wide set of external sources, based on usual authentication and agreed procedures, and is not dependent on third parties' authorisation. When information is requested to other authorities, responses are due by law (and, where applicable, ad hoc MoUs).

In another case, the FIU can ask for or receive from all public entities any information and therefore has access to all information held by other state authorities, which cannot object as long as the request is motivated by concerns relating to money laundering, associate predicate offences or terrorist financing. Accessible information includes data held by tax administrations, among which the national centralised bank and payment account register.

Respondents emphasize the need for a broader range of information available for their functions and for more direct modalities of access.

Despite a general positive feedback, responses highlight that the FIUs' capacity to have access to external sources is subject to conditions and limitations which in some cases can affect their independent action under this important respect.

In several cases, the interrogation of external databases by the FIU is only subject to authentication procedures aimed at ascertaining that the access is performed by authorised personnel and for the exercise of appropriate FIUs' functions, in a framework whereby the independent availability of information for the FIU (either through direct or indirect means) is sufficiently established in law or regulations.

However, it appears that in some instances this access to external sources can be made subject to additional conditions and discretional evaluation by the agency holding the information sought which go beyond mere authentication formalities. These are circumstances where the FIU's access to external sources of information may not be possible under appropriate independent modalities (due to, for example, the lack of dedicated provisions in laws or regulations), with possible repercussions also on the capacity to perform effective analysis or international cooperation.

For example, some respondents highlight that they are subject to specific access procedures, possibly beyond the mere authentication.

More importantly, FIUs may be prevented from freely accessing external sources of information when investigations or legal proceedings are underway on the same cases on in relation to the same information. These are instances where the FIU, rather than independently accessing relevant sources based on its information needs in order to pursue proper analysis, is subject to an authorization or an "agreement" with competent law enforcement agencies.

Others inform that they can obtain information only based on, and subject to, "memoranda of understanding" regulating the cooperation with the agencies holding relevant information.

Other respondents also flag that access to certain sources of information is indirect (as allowed by the Directive) and subject to possible conditions or delays.

Moreover, cases of indirect access are particular widespread and this, coupled with the above mentioned conditions, can also affect FIUs' capacity to freely and rapidly obtain the information needed for the analysis or international cooperation.

2.5.2 Autonomous capacity to request and obtain information from obliged entities

The extent and modalities of the EU FIUs' capacity to obtain information from obliged entities, for analysis and cooperation purposes, will be specifically discussed in Chapter 4. As this is also an essential component of the FIUs' toolkit underpinning their functions, it is important to discuss briefly, in this paragraph, the FIUs' capacity to exercise this power in an independent manner. Independence particularly entails, in this context, that FIUs can request and obtain information from obliged entities without being subject to authorization from third parties that can previously receive and evaluate the FIU's query. This also implies that requests should in principle be filed directly by the FIU the obliged entities holding the information sought.

All FIUs have confirmed, in their responses, that they do have the capacity to request and obtain information from obliged entities without depending on third parties' discretional authorization. In general, national laws explicitly oblige reporting entities to provide data and information to FIUs upon their request.

A respondent informed that obliged entities have to provide the FIU, for the performance of its tasks, with data on transactions and on persons involved in such transactions, upon request of the FIU itself, which also specifies a deadline for the response.

Another respondent has indicated that it can access autonomously and independently the information from any obliged entity, without third parties authorisation, and independently of the source of the original report analyzed as well as regardless of whether a STR has been filed. The requests can pertain to data on customers, accounts, specific transactions or any other type of documentation, specifically (but not exclusively) that obtained in fulfilment of the legislation against money laundering.

Responses also generally highlight that the FIUs' power to obtain information from obliged entities can be exercised under no particular conditions or filters and without depending on third parties' authorisation.

For instance, in one case a FIU has indicated that the reporting entities must upon request, and irrespective of a previous filed STR, immediately provide the FIU with all information it deems necessary to prevent or pursue cases of money laundering or terrorist financing. That means that the FIU can obtain necessary information independently, as long as there is suspicion of ML/TF activities.

An FIU has explicitly indicated that the national law stipulates an "absolute right" of the FIU to request information from reporting entities and that such right is independently applicable with no need for any third parties` discretional authorization. Along the same lines, other respondents have reported that they "can request any obliged entities at any time to obtain information without depending on third parties' authorization" or that they have the power "to request information and obtain information directly from all obliged entities, without the intervention of third parties and that replies to requests for information are submitted by reporting entities directly to the FIU without any third party involvement".

Despite this positive feedback, responses also highlight, in some cases, that conditions and limitations apply to the FIUs' capacity to obtain information from obliged entities. These conditions, that affect both the FIUs' effective operations and their independence status, can be traced back to the following main factors.

- The existence of investigations or legal proceedings on the same or related cases or information inhibits the FIU's capacity to approach obliged entities with requests upon autonomous decisions (an authorization from competent law enforcement agencies may be required)[55].
- In some cases, the FIU's requests to obtain information from obliged entities is made subject to the evaluation of third parties for prior authorization; this is notably the case of authorizations released by courts or prosecutors (regardless of the existence of related ongoing investigations prosecutions), as the access to information held by obliged entities, particularly that of a financial nature, is considered a law enforcement measure, as such beyond the FIU's area of competence.

[55] See also the information and analysis in Chapter 4 on existing limitations affecting this FIUs' power.

- In other instances, the capacity to request information is strictly dependent on the existence of an STR/SAR that was previously reported to the FIU on the same case or subject[56].

For example, the following instances have been reported where a prior authorization is needed for the FIU to request and obtain information from obliged entities.

An FIU may collect data to supplement existing information or for the purpose of analysis by placing requests for information or making enquiries with public and non-public bodies. However, in cases where criminal proceedings are pending, the FIU may exercise this power only in agreement with the competent prosecution authority[57].

Another respondent to the Survey has indicated there are no particular restrictions when it comes to obtain additional information from obliged entities. However, the same FIU affirms that in some cases there is the need to obtain a court order in order to procure the relevant information of interest.

Another FIU has highlighted that where a report is incomplete, the FIU will directly ask the reporting entity to provide the missing information, to make it possible for the FIU to conduct a relevant analysis of the material. Moreover, when the FIU needs to obtain further details or information from third parties, including other entities which have not done any reporting in the specific case, it may be necessary to obtain a court order to protect legal certainty.

Conclusions on the FIUs' autonomous capacity to obtain information from obliged entities

Responses to the Survey clearly point to some significant limitations that affect the EU FIUs' capacity to obtain information from obliged entities under appropriate independent conditions. The main outstanding problem in this area seems to lie in the need for some FIUs to obtain a prior authorization from competent courts or prosecutors in order to be able to approach obliged entities with an enforceable request to receive information. As mentioned, this condition seems to pose undue limitations to both the FIUs' effectiveness in performing their own analyses and to their independence status with regard to the capacity to exercise their functions and powers taking "autonomous decisions", in accordance with article 32(3) of the Directive.

At the same time, besides domestic analysis, the need to receive a prior authorization based on, e.g., a court order to obtain information from obliged entities directly affects FIU-to-FIU cooperation also, in all cases where this information is needed to respond to requests from foreign counterparts.

The requirement to subject the FIU's access to information held by obliged entities to a court or prosecutorial order seems to be rooted in the assumption that such access should stem from law enforcement measures which, rather than on the pre-investigative analysis conducted by the FIU, should be connected with proper investigations and should be therefore "validated" by competent investigative authorities outside of the FIU. This assumption does not seem to find any support in the Directive which, on the contrary, maintains that FIUs should be able to obtain this information specifically in support of their analysis (and related FIU-to-FIU cooperation) which, as repeatedly recalled, is distinct and independent from law enforcement activities.

[56] See, on these limitations, also the analysis in Chapter 4.

[57] Notably, this condition seems to apply broadly to the access of information held by any third party, thus impacting the FIU's independence beyond its capacity to query obliged entities specifically.

It is hoped that forthcoming amendments to the EU provisions on this point will further clarify that FIUs should be directly and autonomously able to obtain information from obliged entities, thus requiring Member States to transpose this requirement into domestic laws without any undue conditions or limitations on the FIUs' capacity to approach obliged entities directly.

An explicit reference in the EU legislation may be necessary, or at least greatly beneficial, to facilitate a correct and uniform implementation of this essential requirement across Member States. EU provisions would also be helpful to dispel the assumption that obtaining information from obliged entities is an investigative tool requiring ad-hoc law enforcement measures and to confirm, on the contrary, that such power has to be independently available to FIUs in support of their analysis.

2.6. Autonomy in cooperation with domestic authorities and other FIUs

EU FIUs indicate in their responses to the Survey that they have the capacity to engage independently and exchange information with other domestic authorities, with no need for authorizations from third parties. The same unanimous responses are provided for the cooperation with other FIUs: respondents confirm that they can equally carry out this cooperation in an independent manner[58].

For instance, a respondent has indicated that it can make use of all its powers without differences, regardless of whether the request is made on behalf of a national or foreign authority.

Another respondent is empowered to make arrangements independently with domestic competent authorities, within a national framework that sets out the basis for extensive cooperation with all authorities involved in countering money laundering and terrorism financing, useful to perform its institutional tasks.

Domestic and international cooperation is conducted by EU FIUs based on their domestic legal frameworks, which generally allows and empowers them to share information with other competent authorities and foreign counterparts. The content and types of this information may obviously vary depending on the counterpart authorities, with STR/SAR being subject to special confidentiality safeguards.

Against their national legal framework, EU FIUs appear to be generally free to entertain domestic or cross-border cooperation in an independent manner. This is often also regulated through bilateral ad-hoc MoUs. However, specifically as regards FIU-to-FIU cooperation, it is important to bear in mind that several limitations and constraints still affect EU FIUs' action, as will be amply illustrated in Chapter 6. These limitations also affect the FIUs' status of independence in this area, for example as concerns their capacity to obtain and exchange information without third parties' authorizations.

2.6.1. Capacity to engage independently and exchange information with domestic authorities

As said, responses indicate that EU FIUs can generally engage in cooperation with other domestic authorities and are able to exchange and obtain information useful to support their analytical functions.

[58] The characteristics and limitations to EU FIUs in entertaining cooperation among themselves will be specifically discussed in Chapter 6.

For example, a respondent to the Survey points out that when it deems that reasons for suspicion of money laundering or terrorist financing exist in relation with a transaction or a person, it may request state bodies, local and regional self-government units, and legal persons with public authorities to supply data, information and documentation necessary for the money laundering or terrorist financing prevention and detection purposes.

Another FIU explicitly indicates that there is no third party that affects FIU's decisions in matters concerning domestic cooperation.

In some cases the capacity to engage independently and exchange information with domestic authorities is subject to some conditions, especially represented by the need to enter into ad-hoc MoUs or agreements with competent counterparts.

An FIU informs that it is empowered to make arrangements independently with all domestic competent authorities. Under the national legal framework, MoUs can be entered into in several instances and for multiple purposes:

- with the aim of facilitating the activities connected with the investigation of suspicious transaction reports, the FIU can conclude memoranda of understanding with LEAs establishing the conditions and procedures for such bodies to exchange police data and information;
- the FIU and LEAs can adopt, on the basis of memoranda of understanding, adequate measures to ensure the maximum confidentiality of the identity of those who make reports;
- on the basis of memoranda of understanding, the FIU conducts an in-depth analysis involving the competences of the sectorial supervisory authorities, which shall supplement the information by supplying further information from their own archives. Aside from cases specifically provided for by the law, further MoUs have been signed by the FIU with domestic Authorities considered relevant for the fulfilment of its tasks, such as the National Anti- Corruption Agency.

Another respondent clarifies that, while domestic cooperation also rests on MoUs with competent authorities, legal challenges may arise in the definition and implementation of such agreements; in fact, MoUs need to be approved by a competent Commission, where the National Data Protection Authority also sits and asks for the inclusion of a long data protection clause.

2.6.2. Capacity to engage independently and exchange information with other FIUs

All FIUs confirm they have the capacity to engage independently and exchange information with other FIUs in carrying out analytical functions, without depending on third parties' authorizations. MoUs can also be negotiated and signed by FIUs autonomously. Importantly, it appears that information is exchanged by EU FIUs always directly with foreign counterparts (by making use of dedicated FIU-to-FIU channels), with no cases reported of interposition of other domestic authorities.

For example, in one case national law establishes that the FIU may exchange directly any kind of available or obtainable information without third parties' clearance and cooperate with homologous authorities of other states that pursue the same purposes, subject to reciprocity also as regards confidentiality of information, and conclude memoranda of understanding to this end. The FIU is also empowered to make arrangements independently with foreign counterparts. The capacity to exchange information and enter into MoUs with foreign counterparts rests entirely on FIU's independent action, with no need for third parties' authorization.

Similarly, another respondent informs that it can independently decide when and to what extent it should engage in cooperation with other FIUs, namely by requesting information needed for own analysis or by providing information, either spontaneously or upon request.

Against this general background, however, the analysis in Chapter 6, based on information provided in responses, will highlight that EU FIUs' ability to engage independently in reciprocal cooperation continues to encounter limitations. These are related, for example, to a limited capacity to access and share particular types of information (e.g. that held by certain obliged entities, financial, administrative or law enforcement data) and limitations in providing the consent for further use or dissemination of the information exchanged, still often dependent on the existence of investigations or legal proceedings.

Moreover, significant cases are reported where FIUs have to obtain an authorization by third parties in order to be able to provide certain information to foreign counterparts. This happens particularly when information has to be obtained by the FIU from other domestic authorities and when investigations or legal proceedings are underway on the same case (in these latter instances, an authorization from the competent judge or prosecutor may be needed)[59]. The need for third parties' authorizations clearly limits the FIU's capacity to provide cooperation under appropriate independent conditions; in fact, in contrast with article 32(3) of the Directive, the FIU is not in a position to "take autonomous decisions"[60].

2.6.3. Autonomous capacity to suspend or withhold consent to suspicious transactions at the request of another EU FIU

The majority of FIUs have highlighted that they have the capacity to suspend or withhold consent to suspicious transactions at the request of another European FIU based on their own decision, without third parties' authorization or validation.

More in detail, according to responses, this postponement power can be exercised by FIUs in an independent manner regardless of whether the decision is taken by the FIU itself in the pursuance of its own functions or is adopted upon a request received from another domestic agency or a foreign counterpart.

As indicated by a respondent, the FIU may dispose, both at the request of the National judicial authorities or upon the request of foreign institutions which have similar functions and which have the obligation of keeping the secrecy under similar conditions, the suspension of the execution of a transaction which may be related to money laundering or terrorism financing activities.

For another FIU, the power of suspension can be and it has been applied in several cases also on behalf of other FIUs and its application always results from an autonomous decision-making process.

The FIU's capacity to postpone or withhold the consent to suspicious transactions (either upon its own decision or on request by foreign counterparts), and to do this under an independent decision-making process, is generally reflected explicitly in national laws which specifically empower FIUs

[59] See Chapter 6, par. 1.8, for more details and examples on this aspect.

[60] This has of course also consequences on the extent of the cooperation that can be lent to foreign FIUs, as will be specifically discussed in Chapter 6.

for this purpose. Nonetheless, there are cases where transactions can be postponed by the FIU also in lack of explicit legal provisions on this point, based on the overall legal framework and to the FIU's role and powers within that framework.

In this regard, a respondent highlights that, as required by the law, at a substantiated written proposal given by a foreign financial intelligence Unit, under the conditions provided for by the same law and on the basis of effective reciprocity, the FIU may issue a written order to instruct a reporting entity to temporarily suspend a suspicious transaction execution for up to 72 hours. The FIU shall notify the State Attorney's Office of the issued order without any undue delay. Reciprocally, within the framework of carrying out money laundering and terrorist financing prevention and detection tasks, the FIU may submit a written proposal to a foreign financial intelligence unit for a temporary suspension of transaction execution, should the FIU judge that there are reasons for suspicion of money laundering or terrorist financing associated with a person or a transaction.

Another FIU confirms that it has the capacity to suspend transactions or block accounts at the request of a foreign counterpart, although this is currently not explicitly stated in the domestic AML/CFT law, based on its general power attributed for postponing suspicious transactions, regardless of whether these are reported domestically or by foreign counterparts.

Importantly, some respondents to the Survey point out that the capacity to postpone transactions on request by foreign FIUs has not yet been specifically implemented in national law, as this was only introduced by the fourth Directive. It is also important to underscore that the Directive, while requiring that EU FIUs should be able to take action to secure a postponement (also upon foreign requests), does not mandate that the decision to suspend should necessarily be taken by the FIU itself; therefore, cases where the decision-making power on this matter is not attributed to the FIU should not be understood to imply necessarily an undue limitation to the FIU's independence (more precisely, such limitation would certainly exist in such cases but this would be in accordance with the Directive).

Although no specific evidence has been gathered on this point through the Survey, cases where the decision to postpone a transaction reported as suspicious to the FIU is taken by a different domestic authorities, upon the FIU's initiative, may raise concerns under several respects. In general, although the postponement power is not formally vested in the FIU, whenever the suspension is not adopted by the competent authority, this would imply an element of limitation to the FIU's own assessment and discretion. As mentioned, especially if contrasting decisions by the competent authority are frequent, the FIU's status of independence may even be at stake. Also mechanisms based on the FIU's initiative for the postponement and the adoption of the order by a third party require a procedure which inevitably takes some time: this could bear risks of inefficiency and untimely decisions. Finally, because of multiple parties involved in the decision-making process, the confidentiality regime of underlying STR/SAR information may be weakened, with heightened risks of undue circulation.

2.7 Autonomy and independence in the FIUs' organisation

FIUs' effective operations and independent and autonomous functions depend critically on the availability of sufficient resources and on the capacity to manage these resources without undue influence or interference from third parties. Lack of resources would prevent FIUs from fulfilling their tasks, despite any formal independence that may be recognised; at the same time, having resources available but not being able to manage them autonomously would also directly affect the FIU's capacity to independently determine and pursue relevant priorities or even achieve set

objectives. These two aspects are specifically dealt with and regulated under the FATF standards and, partly, by the fourth Directive.

Article 32(3) of the latter first recalls that "each FIU shall be operationally independent and autonomous, which means that the FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information". It then establishes that "Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks". Regardless of their nature and institutional setting, FIUs should be endowed with resources that, both in terms of quantity and quality, are commensurate to the range and complexity of their functions. As these functions also evolve in types and articulation, resources should also evolve and increase (in quantity and quality) to support those functions adequately. Sufficient resources should of course be available for discharging the FIUs' tasks regardless of whether the FIU is embedded into a bigger organization and regardless of the level of that embedment.

FATF Interpretive Note to Recommendation 29 also confirms that "the FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively"; it goes further by stating that "the FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence".

3. Adequacy of resources

Based on responses, EU FIUs seem to be under considerable operational pressure and their resources are reported to be under severe strain and stretched to the maximum possible extent. More than half of respondents to the Survey have indicated that additional resources, financial, human and technical, would be needed to continue performing the FIUs' functions in an effective manner. The capacity to give appropriate consideration to all available information may be at risk in some cases, due to the constantly expanding range of data received or otherwise accessible. This can of course affect the quality and timeliness of the analysis, together with the FIU's capacity to identify relevant cases of money laundering or terrorist financing for prompt follow up by investigators or prosecutors.

Respondents have flagged multiple root causes which lie at the basis of the current scarcity of resources. On the one hand, this is due to the considerable increase of the workload. This, in turn, is determined by several factors: current trends of constantly expanding volumes of STRs/SARs; more frequent and numerous exchanges of information with foreign counterparts on cases that have connections with other countries; innovative forms of domestic activities (e.g. inter-agency information sharing) or FIU-to-FIU cooperation deriving from new practices as well as from the implementation of the fourth Directive[61].

A respondent, for example, has indicated that the flow of information (STRs, requests) towards the FIU is steadily increasing, as a result of which more staff has to be employed in the reception of information. The reports from the banks have so far been given an individual treatment and the situation is approaching when this will not anymore be possible. Also, the more information is

[61] Although this is not explicitly recalled in responses to the Survey, FIUs' role has been expanded particularly as a consequence of heightened terrorism threats. The need for more effective prevention, particularly on the financial standpoint, is leading to increasing volumes of activities associated with domestic disclosures and information sharing, as well as in international exchanges of various nature.

received the more personnel will have to be dedicated to the analysis and investigation functions. Similarly, the more the amount of information in the data warehouse will increase, the more the need to analyse the information will grow.

The fourth Directive has expanded FIUs' functions and the powers available for their exercise. It has also increased the complexity and articulation of FIUs' activities. Respondent FIUs have highlighted how some innovations introduced by the Directive will be likely to exert pressure on the organization and resources. These include, for example, the need to perform operational and strategic analysis as two different, though connected, functions; the approach to operational analysis based on the capacity to consider all information and then selectively single out cases and data deserving further follow-up; in international cooperation, the requirement to go beyond the traditional exchanges based on the usual "request-reply" or spontaneous disclosure dynamics (which are also growing) and develop automatic mandatory flows of information in relation to reports that concerns other Member States (article 53(1)).

Clearly, as said, lack of sufficient resources can have an impact on the capacity to consider all information properly and perform effective analysis, which is at the core of the FIUs' functions. As flagged in several responses, EU FIUs demands for additional resources are often declined by competent authorities due to general budgetary constraints, as a consequence of deteriorated economic conditions. Responses on this point emphasize existing difficulties for FIUs, faced with increasing volumes of activities, to obtain additional resources to cope with the workload.

A respondent to the Survey has reported that, as a result of global austerity, the FIU recently lost a number of staff, and currently has a number of vacancies. Proactive steps are underway to both restructure the FIU to meet demands, as well as to recruit more staff.

Another respondent confirms that, due to the economic crisis, it is difficult to increase staff and budget; the request made a couple of years ago was denied by the responsible Minister also taking into consideration the advice of the Minister of Finance.

Of course, the staffing and functioning of FIUs cannot but be considered by national competent budgetary authorities against the background of general economic conditions (especially as regards fiscal constraints and availability of resources) and in the context of overall expenditure priorities to achieve public policy objectives. Nonetheless, it is important that the FIUs' role is recognised as essential in detecting and fighting money laundering and terrorist financing and in providing support to law enforcement, intelligence and prosecutorial activities and that, as a consequence, appropriate priority is given to FIUs' needs in the context of budgetary decisions. This is also essential to fulfil the condition established in article 32(3) of the fourth Directive which maintains that, of course taking account of evolving activities and the increasing workload, "Member States shall provide their FIUs with adequate financial, human and technical resources in order to fulfil their tasks".

Interestingly, while human and financial resources appear to be a critical factor for the effective functioning of FIUs and their increase is generally reported as difficult due to overall budget constraints, several FIUs emphasize that, resources being constant, they are striving to develop working tools and procedures to face the increasing volumes of activities in a more efficient manner. In particular, the introduction and development of innovative and targeted IT instruments and the "automation" of certain stages of data analysis are often recalled by respondents as a means to process the huge and diversified information that becomes available or can be obtained for analytical purposes in a way which allows to provide substantial support to the FIU's staff in screening information and cases.

In fact, respondents to the Survey that have flagged existing lack of resources also emphasize that "further automation of data analysis" is sought and that the FIU is working "to develop and implement a replacement IT system for all involved in the reporting regime".

Other respondents, on the same vein, highlight that "in case additional IT resources were at use, great enhancements to the technical possibilities to increase the analytical possibilities of the FIU could be developed", with considerable efficiency gains and less absorption of human resources.

As highlighted in another response, the ad hoc data management and analytical tool which will be put in place soon "will free up existing personnel for the conduct of duties within the FIU".

Case-management and data analysis automated systems are widely indicated as necessary tools to develop and keep up to date for the management of big and diversified sets of data, to meet FIUs' increasing workload in a cost-effective and time-efficient manner which also allows to consider all available information and focus on relevant cases for analysis and dissemination, precisely as article 32(3) dictates.

The development of IT tools and procedures for managing increasing volumes of data in support of the analysis function seems to be not only a promising perspective for FIUs' capacity to cope with their workload through a more efficient use of their available resources; it also appears as a necessary prerequisite of an effective analysis function, which entails the selection of relevant cases based on the screening of available information[62]. At the same time, and for these same reasons, IT-supported analysis and decision-making procedures reinforce FIUs' capacity to work autonomously and take independent decisions throughout their working cycle, based on objective technical considerations.

One respondent has also recalled how inter-agency coordination and forms of working together can provide opportunities for the FIU to leverage on resources of other agencies. This respondent signals, in fact, that it has "adapted its policy to maintain effectiveness", despite resource scarcity, by working in conjunction "with several partners, using their own expertise in combination with other partners' expertise".

While forms of flexibility based on the use of external staff can provide opportunities of adjustments in case of emerging needs, it shall however be taken into account that, as already mentioned in Chapter 1, lack of own specialized personnel (especially as regards the performance of own FIUs' functions of analysis) and a systematic use of external staff may, at the same time, affect effectiveness and raise issues of confidentiality and use of data (if appropriate clearance limitations and safeguards are not applied).

It is also important to flag that, as highlighted in several responses, scarce FIUs' resources are often distributed across multiple areas of activities carried out by the same Unit, some of which additional to the core FIU's functions[63]. A careful assessment of priorities, by both FIUs and policy makers, have to be conducted in such cases whenever it is recognised that insufficient resources are deployed to perform the core FIU's functions of receiving and analysing relevant information, focussing on significant cases for further screening and dissemination, ensuring smooth cooperation with other FIUs.

[62] See also the considerations on this point in Chapter 5.
[63] See Chapter 1 for a description and discussion on this aspect.

Margins for cooperation and coordination with other authorities in performing other, non-core FIU functions should be identified and exploited with a view to containing the absorption of resources which could then be allocated to core activities.

A respondent highlights in this regard that, while the FIU is in charge of supervisory functions "over all obliged entities to ensure compliance with the entirety of their AML/CFT obligations (…), in so doing the [Law] allows [the FIU] to seek the assistance of supervisory authorities in the carrying out of on-site examinations". The same respondent also informs that, "at present, the prudential supervisor (…) assists [the FIU] in the carrying out of on-site examinations for credit and financial institutions".

3.1 Conclusions on the adequacy of resources

EU FIUs are faced with increased workloads, higher and more diversified types of information and additional, sometimes innovative tasks. This determines that available resources may be, or become, insufficient or inadequate, with potential consequences on the FIUs' capacity to remain effective in providing useful inputs to prevent and detect money laundering and terrorist financing cases and, as a consequence, to operate under appropriate independent conditions.

National policy makers should ensure that FIUs' human and financial resources are adequately increased (in quantity and quality) to maintain effective and independent functioning. In this, the necessary level of priority should be recognised to the role of the FIU in the context of general public policy and expenditure choices.

To properly cope with the increased volumes and the enhanced difficulties associated with FIUs' information and activities, the development and implementation of suitable IT tools and working procedures is also essential. This not only fosters the efficient use of resources (allowing for savings without impacting the quality of the output), but is also conducive to the objective of FIUs being able to process big and diversified volumes of data maintaining the capacity to consider all information in an integrated manner, automate the analysis process and selectively focus on relevant cases.

IT-supported working procedures also reinforces FIUs' capacity to adopt independent decisions, both as regards the identification of priority areas where available resources should be deployed and the inputs provided for law enforcement or judicial follow up. The need to develop adequate working procedures, case management and analytical tools based on dedicated IT instruments in support of FIUs' activities could be taken up at EU level, both by recognising relevant needs and existing practices and by requiring Member States and FIUs to work in this direction[64].

FIUs and Member States should be encouraged to make sure that, for FIUs that carry out multiple tasks, some of them additional to the FIUs' core functions, a careful assessment of priorities is conducted to avoid that essential FIUs' functions are not compromised due to lack of resources as these have been distributed across a range of diversified activities within the same unit.

[64] For example, the reference to the "application of state-of-the-art technologies", currently mentioned in article 56 of the Directive in relation to FIU-to-FIU cooperation, could be expanded and elaborated with regard to FIUs' internal working procedures too.

4. Assignment and independent management of resources

To secure its autonomy and independence, in the course of its activities, an FIU must be endowed with resources on an ongoing basis, exclusively in light of the consideration of its functional needs. More particularly, decisions concerning the amount, type and quality of the resources to be assigned to the FIU must exclusively depend on the objective of making sure that its functions (as evolving over time, in types and volumes) can be discharged effectively and autonomously. In addition, also to safeguard operational autonomy and independence, the FIU should be able to manage the assigned resources taking account of operational needs and priorities, free from any undue political, government or industry influence or interference.

While the Directive does not set out explicitly this particular requirement in a dedicated provision[65], it follows naturally from the requirements that an FIU has to be provided with "adequate financial, human and technical resources in order to fulfil their tasks" and that these tasks have to be carried out autonomously and independently (article 32(3)).

All respondents to the Survey confirm that they receive their resources (human or financial) without undue influence or interference by third parties stemming from political, government or industry priorities. At the same time, as already discussed in the previous paragraph about the adequacy of the resources available, several constraints are reported and described by respondents as regards the FIUs' capacity to obtain the resources required and to manage them based on fully autonomous decisions. Many of these constraints derive from the allocation of essential decision powers on FIUs' resources within the organization where the FIU is located. These same constraints appear to have different levels of intensity; nonetheless, they appear to affect EU FIUs' independence in managing their resources by considerably (and perhaps unduly) limiting it.

A first group of respondents highlight that, although they depend upon external decisions to some extent, they maintain a significant level of independence in setting resource needs, obtaining needed resources and managing them.

Recalling the general status of independence underpinning the conduction of its activities, a FIU indicates that "as regards the autonomous decision in the internal allocation of resources, the Director is in charge of identifying the needs, related for example to the flows of STRs or to policy activities to be covered with proper expertise and skills". The organization where this FIU is located into "satisfies requests for new resources, consistently with its general recruitment policy" and provides the FIU "with sufficient and adequate resources and financial means to ensure the effective pursuit of its institutional tasks".

Another respondent similarly points out that, although the FIU is located within the competent Ministry, the Director of the FIU is in charge of managing duties and that this ensures that the management itself is carried out "autonomously and that any undue influence is avoided".

While, as recalled, the assignment and recruitment of resources for the FIU are decided upon by the parent organization and are based on decision-making powers and procedures of this organization (as they of course also brings budgetary consequences), a respondent to the Survey has indicated that "targeted recruitment procedures are being carried out to take account of the FIU's specificity

[65] Differently from the FATF standards: see Interpretive Note to Recommendation 29, Sections E and F: "The FIU should be provided with adequate financial, human and technical resources, in a manner that secures its autonomy and independence and allows it to conduct its mandate effectively"; "the FIU should be able to obtain and deploy the resources needed to carry out its functions, on an individual or routine basis, free from any undue political, government or industry influence or interference, which might compromise its operational independence".

and needs". This is an instance where, although the budgetary decision at the basis of the recruitment remains with the organization where the FIU is located, the FIU itself can not only influence this decision based on its peculiar operational needs, but can also "target" the recruitment and shape the related procedure, in a way that ensures that staff with the appropriate skills and characteristics can be selected, specifically meeting the peculiar operational needs of the FIU.

Other respondents highlight that they have little or no control or influence over the assignment of resources to the FIU, which is exclusively determined by the bigger organization where they are located. A reduced capacity to manage these resources is also frequently mentioned in responses.

For example, a respondent signals that it has the capacity to take all decisions surrounding the cases it handles, thus being its independent status focused more on operational than organizational issues.

Another FIU indicates that the volumes of STRs/SARs are becoming larger every year, which keeps resources under pressure, whereas the assignment and allocation of resources is not exclusively dependent on the FIU's own decision.

Even more neatly, a considerable number of other respondents point out that FIUs are in no position to decide upon increases in staff or other resources, neither by autonomously recruiting or by otherwise employing personnel based on needs (for example, by extending permissible working hours). All these constraints are dependent on these decisions being reserved exclusively to the organisation where the FIU is embedded.

Responses highlight, for example, that "the FIU is drawn from the resources allocation provided to" the host organization and that it "does not have the autonomy to recruit externally"; it is also underscored that the FIU "cannot make the decisions related to recruitment" and not even "independently decide on the use of its staff", as these decisions "are made by the Head" of the host organization.

Other FIUs indicate that they cannot be "fully independent and autonomous" from the host organization on matters concerning the allocation and use of resources, both because the decision making power rests exclusively within this organization and because the FIU does not have a separate budget.

It is also flagged by other FIUs that "staff working conditions and the designation of new posts cannot be determined by the FIU acting on its own discretion and have to be agreed with government to ensure that they are consistent with civil service policies"; it is consequently recalled that "this process could potentially hinder the capability of the FIU to source human resources and to develop its organisational setup".

The concentration of all decision powers concerning the assignment and use of FIUs' resources within the parent organization may also imply, as flagged by some respondents to the Survey, that this organization not only decides whether staff should be deployed to the FIU, and to what extent, but can also withdraw or divert employees from the FIU and second them to other units in support of activities or projects carried out by these latter. Clearly, the evaluation of priorities in these cases does not take account exclusively of FIU's activities but is based on the consideration of the overall functions of the parent organization (in potential conflict with the FIU's own priorities and their independent pursuance). Also, diverting FIU staff to other, non-FIU, projects may amount to a significant potential interference into the FIU's activities.

Other responses indicate that, while the FIU maintains a certain capacity to propose and request to the parent organization increases in resources, the management of human resources is not flexible enough to allow for quick adjustments, in keeping with the FIU's operational needs.

It is also worth mentioning that, as emphasized by respondents, the lack of independent decision powers on organizational matters extends beyond staffing (and purely budgetary issues). For example, an FIU has indicated that it is not allowed to take decisions on purchasing IT hardware or software.

4.1 Conclusions on assignment and management of resources

The capacity of EU FIUs to obtain resources and manage them in accordance with autonomy and independence requirements appears to be significantly limited. Existing constraints derive from the allocation of decision powers on these matters within the organization where the FIU is embedded.

Although FIUs may maintain some capacity to put forward their needs, requests or proposals, the parent entity remains in charge of all essential management and organization determinations concerning specifically: a) the amount of resources assigned to the FIU (both human and financial[66]); b) the acquisition of new resources, particularly through external recruitment or transfer from other units of the parent organization (as well as the attribution of additional budget); c) the promotion of staff or its appointment to particular positions within the FIU (although some respondents have signaled that they have some room for taking autonomous decisions on these particular aspects); d) the acquisition or development of IT tools in support of the FIU's activities; e) the internal organizational structure, for example through the setting up of internal units or their modification to take account of the evolving context.

The limited capacity of EU FIUs to take autonomous managerial and organizational decisions on their resources and internal structure is thus a consequence of the particularly close link which binds FIUs to the organization where they are embedded. This embedment, although at variable degrees across Member States, brings with it several ties that directly impact on EU FIUs' autonomy and independence.

In light of existing limitations and constraints, as well as of differences of approaches taken by Member States on the FIUs' status of independence, it seems important that the necessary implications of the requirements about "operational autonomy and independence" (only generally recalled in article 32(3) of the Directive) on the FIUs' capacity to manage resources and other aspects of their organization and functioning be properly identified and clarified. EU provisions or indications in this regard would allow, at the same time, to come to a common understanding of these organizational requirements and to ensure that adequate minimum conditions are implemented uniformly and consistently across Member States.

In this respect, targeted work could be devised especially in two directions: reflect the current FATF standards on FIUs' autonomy and independence (see particularly the Interpretive Note to Recommendation 29) into the EU legal framework; further detail these standards by spelling out how EU FIUs should be able to act independently on resources and other organizational matters.

Requirements could be worked out on how FIUs should be able to obtain adequate financial, human and technical resources and manage these resources in an independent manner, without undue

[66] As we have seen in Chapter 1, par. 4.2, FIUs may not even have a separate budget assigned to them in support of their autonomous functioning.

influence by third parties, including the host organization, which may be driven by a different order of priorities. These indications could include, for example, references to processes for recruitment of selected and high skilled staff specifically destined to the FIU. Furthermore, the need for a separate management of the FIU staff and resources with respect to those of the parent organization could be explicitly foreseen. Besides FIU's independence and effective functioning, this would also reassure about the capacity to maintain adequate confidentiality for the information processed in domestic activities and in FIU-to-FIU cooperation.

5. Links with external parties

The operational independence and autonomy requirements established by the Directive apply to FIUs vis-à-vis any third party. This scope includes for example (and perhaps primarily) the relations with the host organization within which the FIU is located. In fact, peculiar challenges may arise for the FIU's independence status especially under two circumstances: a) when the FIU is embedded into a bigger organization which, due to existing close organizational links, may exercise direct powers on the FIU to direct its actions or obtain information; b) in relation to bodies in charge of investigations or prosecutions, who could also be in a position to influence the FIU by directing its analytical work or the exercise of its information powers, as well as to obtain confidential STRs/SARs information.

Limitations to the FIU's operational independence and autonomy appear more likely in situations where, being the FIU an integral part of the host organization where it is embedded, hierarchical links exist between the Head or the staff of the FIU and higher rank officers from such organization, through which the former could be ordered to steer their actions or provide information. Similar links and powers may be exercised on the FIU (either the Head or the staff) in cases where a close relation is established with investigating or prosecuting bodies. The two situations may well coincide, especially for FIUs that are located within law enforcement agencies where analytical and investigative tasks are strictly linked. It is in these conditions that the independence and autonomy requirements have to be specifically implemented and verified.

5.1. Links with the host organization

The vast majority of respondents to the Survey have indicated that they are not conditioned, in their independent and autonomous operations, by existing links with external parties in the bigger organization where they are located. These responses, however, should be considered together with the findings about the constraints that apply to FIUs' resources which, as said, are in several cases assigned by the parent organization (see Chapter 1, esp. par. 4).

For example, a respondent has reported that, based on domestic law, the Head of the FIU is the top-level decision-making body for any decision related to the functions of the FIU (e.g. on STR analysis, postponement, signing of MoUs). These are performed without any interference by external bodies and, namely by the host organization, towards which the FIU has no hierarchical links. The FIUs' activities thus rest on decision making processes that are self-contained and entirely separate from outside parties, entailing the absence of hierarchical links with the staff of the host organization.

On the other hand, several respondents highlight that the FIU is indeed subject to direction or decisions from higher staff belonging to the organization where it is located. Such hierarchical influence can be exercised either on the performance of the FIU's functions or on organizational matters (this latter seems to be the most common instance for these respondents).

For example, a respondent stresses that the FIU staff ultimately fall under the control of the Head of the host organization where the FIU is embedded; due to the existing hierarchical links, this implies that this staff may be subject to decisions from outside of the FIU and (although this has not occurred in practice) may be deployed to other duties.

Another FIU indicates that, according to the national constitution, all public authorities, including the FIU, are subject to the government that can thus influence its organization (without prejudice to the functions, established by law). Similarly, another respondent emphasizes that, while the core functions are exercised independently, matters concerning resources are decided elsewhere in the host organization.

Based on the information gathered through the Survey, it appears that the exposure to hierarchical links and influence from the host organization depends crucially on the level of embedment of the FIU within such organization: the deeper the unit is located in the structure of the latter, the stronger are these links. Correspondingly, FIUs that are located higher within the organization may enjoy more independence and autonomy as a consequence of lesser links with external staff.

5.2. Links with law enforcement agencies and prosecutors

Similarly to the matter described in the previous paragraph, most EU FIUs indicate that they are not subject to investigators or prosecutors who can direct or steer their analytical work as needed to pursue their law enforcement or judicial purposes. This, of course, should not prevent the ordinary functioning of the coordination and cooperation framework where the FIU can be requested, for example, to provide information or conduct targeted analyses on particular aspects which are relevant to ongoing investigations.

Nevertheless some EU FIUs may in certain cases be subject to direction and decisions from investigators or prosecutors.

A respondent to the Survey has noted that in some very limited cases, when the financial intelligence information has been assigned to on-going prosecution, the prosecutor can order the FIU to conduct specific activities for gathering information by means of its powers (based on provisions in the Criminal Procedure Code).

Another respondent has flagged that the FIU's decision making can be reviewed by the judiciary and that a court order may override the FIU's "statutory practice".

5.3. Access to FIU's information by third parties

Operational independence and autonomy requirements are strictly linked with confidentiality safeguards. Hierarchical links and powers may in fact entail the capacity of staff from the host organization, or other outside staff, to access, or otherwise obtain, information held by the FIU concerning STRs/SARs, related analysis and international cooperation. FIUs' information, either coming from domestic disclosures, analysis or international cooperation, should be kept confidential and not shared with external staff, including that belonging to the host organization, outside of course of appropriate inter-institutional cooperation mechanisms.

Several respondents to the Survey have confirmed that they are bound by strict confidentiality measures and that they apply relevant safeguards against access to own information by any third party, including staff belonging to the organization where the FIU is located. This staff is therefore prevented from directly accessing FIU's information. This issue, besides being an essential element

qualifying FIUs' independence status, should be considered in conjunction with the protection and security regimes generally applicable to FIUs' information (see Chapter 8).

On this note, a respondent clarifies that personnel outside the FIU can neither influence internal decisions nor access FIU's own information. External staff can in no way access or obtain information on STRs, other information available to the FIU and its activities related to receipt, analysis, dissemination and international cooperation. Full confidentiality is ensured and applied also, based on the law, vis-à-vis the host organization, its staff and hierarchy.

Another FIU stresses that its information is covered by a rigid confidentiality regime established by the law, which also determines cases where the information can be shared with external parties. By law, this FIU is under an explicit prohibition "to communicate the collected data, information and documentation and the course of action on the basis of the [AML/CFT] Law to persons to which data, information and documentation or action shall pertain, or to third persons".

Another example is given by a respondent that emphasizes that, based on the law, the Head of the FIU, the board members and staff of the FIU, as well as other public servants who may be aware of the FIU investigation must not disclose to any third person any information related to receipt, analysis, dissemination and international cooperation.

It is important to recall, though, that while free and direct access by external parties to FIUs' information would represent an unduly breach of confidentiality and independent management and operations of the FIU[67], information deriving from STRs/SARs and related analysis can well be shared by the FIU with competent agencies (this happens typically through dissemination). In keeping with confidentiality and independence conditions, however, this sharing should be based on the FIU's decisions and in appropriate circumstances. As allowed by the Directive, several respondents, in fact, recall that access to own information can be granted to external parties based on the FIU's decision and applicable criteria. This is the case, for example, of dissemination, either spontaneous or upon request from entitled external agencies[68].

An FIU highlights that, while in principle no competent authority or third party has access to FIU's information unless the FIU so allows out of its own volition, such information can be provided by the FIU (spontaneously or upon request) to competent authorities, namely the Police and supervisory authorities, in accordance with the relevant provisions of the AML Law.

Similarly, another FIU notes that it can provide information in response to requests from specific law enforcement agencies; different agencies have separate request conditions and can receive a different range of information.

In one instance, a respondent stresses that it can provide its own information upon request from domestic agencies, with the following notable exceptions: hard copies of STRs; the identity of the reporting entities (except if the reporting entity is itself the target of a judicial proceeding); information obtained from foreign counterparts.

Other responses seem to refer to situations where, even beyond cases of dissemination as recalled above, the FIU's information can be accessed or obtained in a broader manner by third parties,

[67] See also considerations on this aspect in par. 7, par. 3.4.

[68] See specifically on this point article 32(3),(4),(5) of the Directive. The issue of dissemination, especially upon request, is specifically dealt with in Chapter 5 of this Report.

particularly from the organization where the FIU is located and in relation to investigative activities. These instances are normally accompanied by specific requirements or restrictions.

A respondent FIU refers to access regulated through ad-hoc accreditation and criteria: external officers can have direct access to FIUs' information but they need to be accredited against criteria overseen by the FIU. STRs can be transformed into sanitised intelligence reports and sent to non-accredited officers as long as the source of the information is fully protected.

Another FIU, while indicating that access by external parties is provided, clarifies that this happens under strict guidelines and for intelligence purposes only.

In another case, access to FIU's information (specifically STRs and threshold-based reports) is possible for Prosecutors and Courts when investigating circumstances vital for the protection or forfeiture of proceeds, in accordance with the provisions of the law regulating criminal proceeding.

5.4 Conclusions on links with external parties and access to FIU's information

Responses to the Survey show that the requirement that FIUs should be able to take "autonomous decisions" on matters concerning the exercise of their functions and powers, as stated in the Directive, is not properly implemented in situations where the FIU, being embedded in a bigger organization, is subject to hierarchical links with the latter.

Limitations to the FIU's independence concern both the performance of core functions and the capacity to manage resources and organization. These limitations appear to be more significant for FIUs that are embedded more "deeply" within the host organization (that is are located under the responsibility of other units, directorates or departments), as the level of autonomy decreases accordingly. Equally, limitations to the FIUs' independence seem to arise in cases where, outside of ordinary national cooperation and coordination mechanisms, the FIU can be ordered by law enforcement agencies or prosecutors to perform specific analysis or acquire particular information or are otherwise instructed on priorities to pursue.

Repercussions are noted also on the access to information which, beyond the ordinary dissemination mechanisms, may be directly available to staff outside of the FIU (through direct access or acquisition by order, either by staff from the parent organization or by law enforcement bodies or prosecutors).

Against this background the following lines of action should be considered to ensure that EU FIUs fulfil appropriate autonomy and independence requirements.

- A better national implementation is needed to secure that the FIU's is duly isolated, even within the host organization, from undue hierarchical links which may extend to organization and operations matters or translate into influence on activities or priorities.

- Dedicated indications at the EU level, for example through targeted amendments to the provision in the Directive, could explicitly set out a common requirement for Member States to ensure that FIUs maintain their autonomy and independence specifically with respect to the host organization where they may be embedded[69].

[69] Once again, the current FATF standards set out on this point in the Interpretive Note to Recommendation 29 seem to provide an useful starting point.

- Particularly with respect to possible cases of undue influence exercised on the FIU by domestic law enforcement agencies or prosecutors, clarifications on the nature of the FIU's analysis function, being distinct and separate from investigation and research of evidence to be used in legal proceedings, could be helpful[70].

- Similarly through better domestic implementation and targeted common rules at the EU level, an increased focus should be put on the confidentiality regime of the information held by the FIUs, particularly as regards the need to avoid undue access or sharing with third parties outside the ordinary dissemination mechanisms, particularly with respect to the authority where the FIU may be located.

[70] This same point on the need to recall the differences between "analysis" and "investigation" has been mentioned in Chapter 1, on FIUs' different nature and status, and in Chapter 5, in relation to the characteristics of analysis. It will also be discussed in Chapter 6 when dealing with the implications on FIU-to-FIU cooperation.

CHAPTER 3

INFORMATION RECEIVED, AVAILABLE AND ACCESSIBLE TO FIUs

1. Introduction. Disclosures received on suspicious activities

Pursuant to article 33 of the Directive, all EU FIUs receive disclosures filed by obliged entities concerning cases where such entities "know, suspect or have reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing".

Despite the obligation to detect and report suspicions of criminal activities being one of the fundamental cornerstones making up and sustaining the anti-money laundering and, then, counter-terrorist financing system in the international and European framework, this provision has essentially remained unchanged in the more than 25 years of development of the EC and, then, EU legislation in this matter, save for some limited adjustments and updates[71]. Clearly, it does not delineate a common notion of "suspicious transactions" that should be reported to FIUs to feed their analyses. In fact, the fourth Directive lacks a definition of "STR" and a description of its content, thus leaving Member States without a common approach in this matter.

Both the triggering elements and the content or structure of the disclosures are entirely left up to Member States to determine, with only some general indications in the Directive on the former[72]. While the notion of "suspicious transaction" remains undefined as to what a "suspicion" consists in and the information content of the disclosures, a certain level of detail is provided about what such suspicions should particularly focus on: article 33 of the fourth Directive refers to "funds" that are either proceeds of "criminal activity" or are related to "terrorist financing". Both "criminal activity" and "terrorist financing" are defined in article 3 of the Directive. The former notion sets out the minimum scope of crimes that should constitute predicate offences for money laundering.

[71] Article 6 of the first AML Directive, n. 91/308/CEE, read "Member States shall ensure that credit and financial institutions and their directors and employees cooperate fully with the authorities responsible for combating money laundering: - by informing those authorities, on their own initiative, of any fact which might be an indication of money laundering, - by furnishing those authorities, at their request, with all necessary information, in accordance with the procedures established by the applicable legislation". The second Directive 2001/97/CE confirmed this minimum harmonization approach, which was also maintained by the third Directive 2005/60/EC (that extended the scope to suspicions of terrorist financing). This same provision is now replicated, with few adaptations, in article 33(1) of the fourth Directive (EU) 2015/849: "Member States shall require obliged entities, and, where applicable, their directors and employees, to cooperate fully by promptly: a) informing the FIU, including by filing a report, on their own initiative, where the obliged entity knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, and by promptly responding to requests by the FIU for additional information in such cases; and b) providing the FIU, directly or indirectly, at its request, with all necessary information, in accordance with the procedures established by the applicable law".

[72] Three psychological status are referred to, with little hints on differences and implementing details: "knowledge", "suspicion", existence of "reasonable grounds to suspect".

While clearly the identification of suspected money laundering activities rests on the perception that funds derive from illegal activities, it is important to avoid an expectation that obliged entities, in the effort to detect anomalies in the exercise of their respective professional activities, should be able to ascertain that a particular type of crime (specifically one of those comprised in the national list of predicates for money laundering) has been committed and identify that crime in the disclosure to the FIU[73].

As a consequence of the lack of detailed indications in the Directive on the "suspicious transactions" or "suspicious activities" reporting obligation, Member States have taken different approaches to the determination of triggering factors, structure and information content of this obligation. Different types of disclosures have been introduced, variably named "Suspicious Transaction Reports" (STRs), "Suspicious Activity Reports" (SARs) or "Unusual Transaction Reports" (UTRs). To differences in names correspond differences in nature, substance and content. Equally, relevant triggering factors vary significantly across countries, as the notion of "suspicion" is differently defined (and qualified by guidance or indicators), ranging from the identification of mere anomalies to the detection of well-grounded and substantiated criminal behaviors. This has an impact also on the volumes and contents of disclosures received by EU FIUs.

Existing differences in structure and content of disclosures concerning suspicious activities or transactions can also be traced back to some other factors, as described below.

In terms of scope and range of the information which should be included in suspicious transaction reports, these may vary depending on the existence of other disclosures that the same FIU receives or on the extent of the information powers the FIU can exercise to obtain additional information as needed for the analysis of the disclosures received. For example, an FIU can receive relatively few STRs/SARs but still maintain an adequate analytical capacity because the "pool" of information available is also fed by other, threshold-based disclosures (see paragraph 3). Or, the information content of STRs/SARs may be relatively simple or reduced because it is considered that, rather than requiring obliged entities to provide ample information upfront, it should be left up to the FIU to request additional information (either from the same obliged entities or from other sources) when, and to the extent that, this is specifically needed for the analysis.

The opposite may be of course equally true: FIUs that receive a significant volume of initial disclosures (STRs, SARs or threshold-based disclosures, in different proportions) may have a lesser need to obtain additional information using available powers as needed for the analysis.

While this somehow "idealized" picture seems to emerge clearly from the provisions in the Directive related to the reporting obligations, the FIUs' receipt function and the powers to obtain information (as well as from the FATF standards on the same matters), the survey gives a different picture of what happens in practice in relation to the "mix" of tools variably used in Member States to ensure that FIUs have an adequate range of information available for their analyses.

While there is no evidence that the different information tools used in Member States are in all cases well balanced and result in FIUs having an adequate range of information available, differences in FIUs' capacity and powers, as said, are likely to affect the type and quality of the

[73] As discussed elsewhere in the Report, (see particularly Chapters 5 and 6), not even the FIU, in discharging its analytical functions on suspicious activities should be expected to establish the commission of particular types of criminal activities and find related supporting evidence, as this will result, after dissemination, from ensuing law enforcement or judicial activities.

analyses performed by different FIUs and also their capacity to provide cooperation.

It is important to note that some of the differences in the structure and content of disclosures received are also dependent on the different objectives underlying the analysis functions that FIUs are in charge of. For example, FIUs that focus more on police activities may be more interested in linking the reported facts to possible predicate offences and less oriented towards obtaining and assessing detailed financial data (with respect to, for example, information on places, dates and movements of involved individuals). Whereas, on the other hand, FIUs that are more focused on the analysis of unusual or anomalous behaviors may depend more heavily on financial information.

1.2 Money laundering and "associated predicate offences"

It is also important to recall that the fourth Directive establishes that FIU are responsible for receiving and analysing suspicious transaction reports and other information relevant to, besides money laundering (and terrorist financing), also "associated predicate offences" (article 32(3)). The same scope, inclusive of suspicions of "predicate offences", is reflected in the configuration of the obligation to report: this becomes due when reporting entities know, suspect or have reasonable grounds to suspect that funds are the proceeds of "criminal activity" (or are related to terrorist financing), which is in fact defined in article 3(4) of the Directive by reference to the underlying predicate offences.

Although this point has not been specifically covered by the survey, responses seem to show that national laws generally refer to money laundering and terrorist financing as relevant sources of suspicion, without specifically and separately mentioning, for the former, the "associated predicate offences" or the underlying "criminal activity" originating the detected proceeds. However, even in the absence of an explicit reference to predicate offences or underlying criminality, the reporting obligation should certainly include (for suspicions of money laundering) references to proceeds potentially deriving from criminal activities, regardless of whether these proceeds are detected upfront, that is stemming from a particular possible offence, or downstream, that is in a subsequent money laundering phase.

What is important is that, regardless of whether "predicate offences" or money laundering is referred to as the source or objective of suspicions and related disclosures, obliged entities report, and FIUs receive, information regardless of whether the suspicious case is considered to concern money laundering or a particular predicate offence. More specifically, the duty to report and the FIUs' functions, as they lie at a stage of suspicion and analysis, should not be conditioned by the identification and nature of underlying predicate offences, which is rather a concern for subsequent investigations or legal proceedings. This is particularly important when it comes to defining the scope of the reporting obligation (reporting entities should not be required to identify particular crimes) and the nature of the FIUs' analysis (as well as the scope of the related FIU-to-FIU cooperation)[74].

2. Nature and use of disclosures on suspicions: STRs, SARs, UTRs

Against the background of article 33 of the fourth Directive and of the lack of a detailed definition of the disclosure of suspicious activities, the approaches taken by Member States to defining "STRs" differ along essentially two axes: the nature of the disclosure and its format and content. On

[74] As regards FIU-to-FIU cooperation, these points will be more amply discussed in Chapter 6. See also article 53 of the Directive which states that the exchange of information should not be conditioned by the indication and nature of possible predicate offences.

the former aspect, disclosures are differently regulated, and accordingly termed, as "Suspicious Transaction Reports" (STRs), "Suspicious Activity Reports" (SARs), "Unusual Transaction Reports" (UTRs). Under the second respect, the information content varies to take account of both the analytical needs and the type of reporting entity and of the activities performed.

The vast majority of respondents have indicated that they receive disclosures in the form of STRs[75]. Only few respondents have referred to SARs or UTRs. The differences among these types of disclosures do not seem to be particularly significant and should not be overestimated. In terms of the information content, while STRs focus in principle on specific "transactions" and on the associated anomalies, the scope of SARs is broader as it extends beyond individual transactions and encompasses broader behaviours and operations, considered in their entirety to identify potential links with illegal activities[76]. However, responses clearly show that these general differences in the approaches underlying the two types of disclosure are to a great extent compensated by the respective information content of STRs and SARs, which is significantly convergent. In fact, while disclosures labelled as STRs generally include information on the overall operational context surrounding the transaction or the subject which is specifically reported, SARs, on the other hand, focus on particular transactions (or subjects) that have to be identified and described[77].

For example, a respondent to the Survey points out that the disclosures, filed as "SARs", "include data on [i.a.] the transaction history". On the other hand, similar to other respondents that receive STRs, an FIU clarifies that "the STRs include (…) indications on the suspicious activities carried out, on the accounts or other relations involved, on the transactions carried out and on those linked to the suspicious one detected, including other subjects connected".

Generally, therefore, both STRs and SARs focus on individual transactions identified as specifically suspicious and at the same time include information on the contextual operations and on connections with relevant activities or subjects.

As regards Unusual Transaction Reports, the difference with respect to STRs and SARs seem to be one of nature and relevance, more than being related to the content. While, based on responses, this latter does not seem markedly different in UTRs compared to other types of disclosures falling under article 33 of the Directive, reports on "unusual transactions", first of all, may be triggered by specifically dedicated indicators set by competent authorities: the disclosure does not feature outright or full-fledged suspicions and rather stems from the identification of anomaly factors in line with applicable indicators.

This "UTR" approach to setting the scope of the duty to report cases to the FIU under article 33 of the Directive provides a telling exemplification of how broad this provision is and how it can accommodate different, equally legitimate and valid, solutions adopted at national level. In line with the prerequisite that the disclosure become due when either "knowledge", "suspicion" or "grounds to suspect" occur, it may well be established, as in the case of disclosures in the form of

[75] Some have made reference to both STRs and SARs as equivalent notions of the same type of disclosure.

[76] In this regard, a respondent notes that "suspicious activities" may not involve an actual transaction: for example, in case of an account holder who regularly changes the address in a short time, the reporter may become suspicious and file a report even if there is no transaction involved. "Also, certain sectors do not consider the issue on which they are reporting to be a 'transaction'. For example, a legal firm reporting on a company buy-out or take-over do not consider that to be a transaction".

[77] Even in cases where no transaction is performed (for example, when this is simply attempted or when the suspicion stems from other aspects of the customer's behaviour, such as the reluctance to provide information at the outset of a business relation with a non-financial business or profession, regardless of whether this relation is started or not), STRs are normally equally due.

UTRs, that the reporting obligation is triggered by anomalies identified based on a set of pre-determined criteria which are found to be met by particular operations or transactions.

As said, while the UTR approach to the disclosure of "suspicions" seems to be firmly rooted in article 33 of the Directive as one of the possible solutions allowed for national implementation, it also determines difficulties when it comes to international cooperation. In fact, responses show that UTR information may not be available for FIU-to-FIU exchange (at least, not until the disclosure is further examined by the FIU and the case is found to be "suspicious").

Similarly, UTRs may not be considered as "cross-border STRs" for the purpose of article 53(1) of the Directive and, therefore, neither forwarded to interested FIUs nor made subject to, or utilised in, joint analyses.

In this regard, the findings reflected in a FATF Mutual Evaluation of a EU Member State where the obligation to file UTRs is in place can be recalled as an example. In this particular case, UTR data is covered by a high level of confidentiality and, being classified as "personal data", is subject to restrictions to possible use that are more stringent than those applicable to STR information. In international exchanges, while the information of "whether the requested person is in the UTR database" can be provided, the contents of these disclosures may not be available for sharing. The exchange can only be achieved by indirect means: "In order to be able to provide information from the UTR database (…), the FIU transforms automatically the request received from foreign FIUs into STR", which allows for a broader spectrum of information to be forwarded.

As regards the relevance and use of UTRs, differently from STRs and SARs, they usually do not trigger the full analytical toolkit of the receiving FIU. This, in fact, only submits these disclosures to preliminary consideration to determine if, in light of subjective and objective elements and other information available, the underlying cases or activities reach the threshold of true "suspicion" or not. Only in the former case a full-fledged analysis is started by the FIU, whereas in the latter the disclosure is set aside (and possibly further considered in future in case of matches with additional intelligence or newly received disclosures). In this, the treatment of UTRs resembles to some extent that of threshold-based disclosures: as discussed in paragraph 3 below, information received through these disclosures is also used by FIUs in support of their analysis but is not considered relevant per se as an autonomous indication of suspicious facts.

In any event, it is also true that, similar to the consideration of UTRs under the FIU's preliminary scrutiny to determine if they qualify for proper analysis of genuine suspicions, several FIUs that receive STRs or SARs also indicate that they approach these disclosures under a phased approach. Especially when the number of reports is considerable, to ensure that cases are properly selected and prioritised, STRs and SARs can be made subject to a preliminary scrutiny which, more than an analysis geared towards the identification of money laundering or terrorist financing activities, consists in an assessment of their potential relevance to distinguish cases which deserve closer or immediate attention from those that may not qualify as genuinely suspicious, in light of information available to the FIU and to relevant scoring criteria. Similarly to the treatment of UTRs which become STRs and are made subject to full analysis after "validation" by the receiving FIU, also in such cases STRs and SARs are preliminarily reviewed to determine if they deserve in-depth consideration through a complete analytical process or can be set aside as not immediately relevant.

The features of the analytical functions discharged by FIUs are discussed in details in Chapter 5, where the approaches based on initial selection followed by in-depth targeted analysis are also recalled and the capacity of FIUs to focus on relevant cases is illustrated[78].

The need to allow for this layered approach to the consideration and analysis of STRs, based on appropriate selection, may be reflected in the structure and content of the disclosures themselves. On this note, an FIU highlights that "the reporting entity assigns a risk level to the transactions reported using a scale from 1 (lower) to 5 (higher)". Moreover, "the STRs loaded [in the FIU's case-management system] can be immediately analysed after the assignment of a provisional risk rating which entails the level of prioritization".

2.1 Structure and content of disclosures

Different types of disclosures filed to FIUs, besides varying in nature and use, also carry different contents, although several significant commonalities can be identified. Similarities can be found particularly in the structure of disclosures, as they all feature some essential constituent elements. Based on the responses received, common information making up the structure of disclosures, across different systems and approaches, include, for example, the identification of the reporting entity (often enriched with contact details of the responsible reporting unit or officers) and the description of subjective and objective elements surrounding the suspicious or anomalous activities detected (e.g. identity data of involved subjects and related beneficial owners, transactional information), together with references to grounds for suspicion. The information elements that are most commonly found in disclosures filed to FIUs, as resulting from the responses, are summarised in the following box.

Common structural elements in disclosures

- Data on the reporting entity
- Data on the reported customer(s) (detailed ID data or ampler KYC/CDD information)
- Data on the beneficial owner
- Information on the activity or transactions detected as suspicious
- Indication and description of the business relationship(s) involved
- Description of the grounds for suspicion or indication of the applied indicators or criteria

Against these essential common elements, what varies significantly in the structure of disclosures across national approaches is, on the one hand, the more detailed articulation which in some cases includes dedicated and extensive references to the characteristics of the suspicious activities detected, the description of the underlying reasons which underpin the suspicion, the overall description of the operational context in which the suspicious activities have taken place and of connections with other subjects or activities.

Examples of areas of further articulation of disclosures

- Beneficiary(ies) of the reported transactions or recipients of the funds or assets involved
- Financial amounts involved in reported activities and types of instruments or assets
- Number and status of relevant transactions
- Details of cash deposits and withdrawals, incoming and outgoing wire transfers, banks

[78] See particularly paragraphs 2.4 and 2.5 in Chapter 5.

cheques (issued or cashed)
- Data on accounts or other relations involved and on linked transactions and subjects
- Activity which the natural or legal persons participating in transactions are known to engage in, and the congruence between this activity and the transactions made
- List of transactions and their dates, nature, currency, amounts, places involved, purpose and means of payment or collection used
- Statement of all circumstances giving rise to the suspicion or evidencing the lack of economic, professional or business justification for the activities carried out.

Elements of flexibility in the structure and content of the disclosures as well as in the ways in which they should be filled in are always ensured. This is needed, on the one hand, to account for the considerable variety of categories of reporting entities, which brings with it differences in the types of activities reported as suspicious or anomalous and in the involved or connected subjects. On the other hand, flexibility is also necessary to ensure that the structure of the disclosure format is able to accommodate different cases and different ranges of information available in each particular instance to reporting entities, as well as the need for them to highlight relevant elements to properly characterise the activities detected and the underlying grounds for suspicion.

This flexibility in structure and content of disclosures is achieved through different but complementary means: the information fields in the reporting formats may not be all equally mandatory and can be filled in depending on the circumstances, the types of transactions and the subjects involved. Moreover, the information content may not be rigidly pre-determined and, in some cases or in some parts of the disclosure templates, reporting entities may be required to include either textual description or narrative as needed to illustrate the particular case identified or structured information or data concerning transactions carried out, amounts involved, connected subjects[79]. In some cases, additional information or documents which may not be included in the structure of the disclosure are required as annexes.

Responses clearly demonstrate that the structure and contents of disclosures filed to EU FIUs, in the forms of either STRs, SARs or UTRs, vary to a considerable extent. Although there are commonalities, significant differences exist. These are clearly not only related to the format but affect the type and extent of the information which is made available to FIUs in different countries as well as the level of details on particular aspects concerning the activities detected, the operational context, the subjects involved, the grounds for suspicion.

2.2 Implications for the FIUs' analysis (and international cooperation)

As already highlighted, the FIUs' analytical activities are closely dependent, in their features, extent and objectives, on the types and range of the information received through the disclosures, as well as of course on the FIUs' capacity to obtain additional elements by accessing own or external databases or exercising information powers. As also highlighted, differences in disclosures are reflected in differences in approaches by FIUs to the analytical functions, as these are characterised by variable objectives and capabilities. The capacity to provide international cooperation and its extent is affected too. The same issue can of course be pictured under a different perspective: it is the nature and objective of the analysis function assigned to the FIU (e.g. as to whether it should

[79] While in most cases a common structured template is made available to reporting entities, some respondents have indicated that "all information available or accessible which leads to an STR must be reported" as there is "no fixed structure" for STRs or, in another case, that "a blank SAR template" is provided and that "the content of the report/free text fields is a matter for the reporter"; all disclosures are accepted "as long as certain standards are met".

aim at pure pre-investigative financial analysis on anomalous economic behaviours or should rather directly point at investigative results) which define the types and content of the information that should be fed to the FIU through disclosures or otherwise made available to it through access to other sources.

As regards the structure and content of disclosures, and the way in which these can shape or influence the analytical function of the receiving FIU, the following considerations can be developed.

- **Disclosures based on in-depth scrutiny by the reporting entity on customers' behaviours, on the elements of suspicion and on a broad set of information and documents resulting from CDD and other monitoring**. When the information content required for filing STRs/SARs is particularly articulated, the timeframe for filing reports may be relatively longer, due to the need to complete the necessary scrutiny and gather all required elements. At the same time, a richer set of information allows the FIU to immediately assess the case, assign the appropriate priority and start the analysis, with no or limited need to request additional information (from obliged entities or other external sources), with the associated delays. Also, the quality of the FIUs' assessment and analysis is expected to be relatively higher, thanks again to the comprehensive set of information provided in the disclosure on the detected suspicions and the relevant context.

- **Disclosures based on "simplified" examination by the reporting entity, also relying on objective indicators, and containing basic references to the case**. These are cases where rapidity in the disclosure may be favored over comprehensiveness and where, as a consequence, the FIU is in a position to receive quick inputs but may have relatively more difficulties in following these up by appreciating fully the significance of the case without resorting to additional information. In the same spirit of rapid reaction, in these cases the FIU may opt for a quick dissemination to competent law enforcement agencies, which can attach to the disclosed inputs an immediate investigative value, rather than embarking in lengthy financial analysis which would imply, in most cases, retrieving information from other sources. In addition to being rapid, these more "simplified" disclosures are usually more numerous: this is one more reason for the FIU to disseminate quickly, based on a "light" analysis (for example, focused on finding connections with data already available or easily obtainable), in the intent to facilitate possible law enforcement results.

The structure and information content of disclosures is also associated and aligned with the nature and objectives of the analysis. FIUs that tend to shift towards a law enforcement-type of analysis[80] normally avail themselves of disclosures that are centered around the identification of particular subjects and transactions[81] and their involvement in investigations or connections with investigated subjects. Consistently, these information and disclosures are rapidly shared by the FIU through dissemination to competent law enforcement bodies which, beyond the FIU's analysis, can immediately further cross-check the data and develop the intelligence through proper investigations.

For instance, a respondent to the Survey has indicated that as soon as a disclosure is submitted to the FIU it is put onto the FIU internal database; the FIU analyses the disclosures to identify possible matches with specific keywords and subjects of interest lists, to extract strategic and tactical

[80] See Chapter 5, par. 2.2, for a discussion on how "analysis" and "investigation" may overlap for some FIUs. The consequences that this issue brings for FIU-to-FIU cooperation are discussed in Chapter 6.

[81] Based on responses to the Survey, subjective information may extend to, for example, the occupation or employment of the suspects.

intelligence, and makes all disclosures available to law enforcement agencies for investigation. Disclosures are made available to law enforcement within seven days of FIU receipt via a secure online portal through which end users access the FIU's database.

On the other hand, disclosures carrying more articulated information on, e.g., the operational context within which the suspicion has arisen, the economic background of the subjects involved or the associated networks of interest, lend themselves to analyses that are more focused on the underlying economic and financial anomalies, aimed at validating or discarding such anomalies, rather than at drawing conclusions or acquiring potential elements directly indicative of outright criminal activities (this task is entirely left to ensuing investigations).

Like domestic analysis, also international cooperation can be directly affected by the type and the information content of the disclosures received on suspicious activities. Quite intuitively, the FIUs' capacity to provide information (in response to requests, on a spontaneous basis or through mandatory cross-border STRs/SARs) is influenced by the information that they have available through initial disclosures. In principle, the broader and more detailed the scope of this information, the ampler and quicker will be the capacity to provide cooperation. More articulated initial disclosures facilitate the identification of connections with other countries and minimize the need to access external sources to obtain the information requested by a foreign counterpart, to the benefit of timely responses.

On the other hand, as detailed disclosures may be less numerous or reported less promptly, the likelihood of identifying matches with incoming foreign requests may be lower than in cases where more disclosures are received, although less rich in their content. In essence, the following considerations can be developed on this point.

- **STRs based on extensive scrutiny by the reporting entity on the elements of suspicion and a comprehensive set of information and documents.** This approach is likely to generate relatively fewer disclosures and, therefore, less "hits" with foreign requests; on the other hand, when matches are found it is more likely that the information in the disclosure (if up to date) is sufficient to quickly satisfy the request for cooperation.

- **Disclosures based on a simplified scrutiny by the reporting entity and carrying basic information on relevant subjective and objective elements**. Under this approach, as more disclosures are likely to be generated, the probability of positive hits with requests from foreign FIUs is higher. At the same time, however, the FIU's capacity to provide information is generally more limited due to the simplified content of the disclosures, with the consequent need to access other sources for obtaining the requested data. In the perspective of international cooperation, it is important, in these systems, that the FIU is adequately empowered to obtain information, both from external databases and from obliged entities.

2.3 The reporting procedure: direct or through third parties

Like the previous third Directive, the fourth Directive allows Member States to provide for limited derogations to the general rule that STRs/SARs should be filed directly and exclusively to the FIU[82]. Article 34 foresees that, by way of derogation, some categories of obliged entities, namely lawyers, auditors, external accountants, tax advisors, notaries, and real estate agents, can be allowed

[82] This rule is set out in article 33 of the fourth Directive.

to file their disclosures concerning suspicious activities to an "appropriate self-regulatory body of the profession concerned", as specifically designated for this purpose[83].

The derogation to the direct reporting to the FIU impinges upon the core FIU's function of receiving STRs/SARs which, besides being reflected in article 33 in the perspective of the obligation to disclose for reporting entities, is enshrined in the definition itself of "FIU" set out in article 32(3)[84]. As the FIU's analytical capabilities are, to a large extent, a function of the information received through STRs/SARs, it is important that also in cases of indirect reporting through designated self-regulatory organizations, the information is ultimately forwarded to the FIU promptly and unfiltered. These are precisely the conditions that, based on article 34 of the Directive, have to be fulfilled by Member States that intend to introduce or maintain forms of indirect reporting as a means of encouraging disclosures from certain categories of obliged entities.

Responses to the Survey show that forms of indirect reporting are allowed in very limited cases and circumstances. Whilst the vast majority of FIUs confirm that the disclosures are filed directly to them, only three respondents have referred to systems of indirect reporting, allowed for certain categories of professions through their respective self-regulatory bodies.

On this note, an FIU flags that "certain categories of DNFBPs (i.e. notaries, labour consultants) send the reports to their professional associations, which in turn transmit it electronically without delay to the FIU". Another respondent informs that financial institutions and other entities must report suspicious operations or transactions "to the FIU and advocates or advocates' assistants to the Bar Association (the Bar Association communicates the information to the FIU not later than within three working hours)". One response highlights that disclosures are "generally done directly" and that "legal professions can make use of a (internal) third party for checks and advise in order to report" (it seems, therefore, that the disclosures are forwarded by lawyers, following this internal consultation, directly to the FIU).

These responses seem also to confirm that the disclosures received by the interposed bodies are promptly forwarded to the FIU, normally through dedicated electronic means. In some cases, however, it appears that the disclosures may be made subject to some forms of filtering by the self-regulatory body, which may decide that particular STRs/SARs should not be forwarded to the FIU (for example, because these are not deemed to be properly substantiated or the reported activities are not considered suspicious).

In this regard, a respondent has indicated that "lawyers must first report to the dean of the law society who will then decide whether the STR must be continued" to the FIU.

While, therefore, it appears that the reporting procedure may be in some cases discontinued by professional bodies that decide not to forward disclosures to the FIU, responses do not allow to determine whether other forms of filtering can be performed by these bodies, specifically on the content of the STRs/SARs channelled through them. For example, information on the reporting professional who initiated the disclosure or on subjects involved in the reporting activities may be omitted to protect professional secrecy or privilege.

[83] The rationale underlying this derogation to the general rule of direct reporting to the FIU is explained, at least partly, in Recital 39 of the Directive: "in accordance with the case-law of the European Court of Human Rights, a system of first instance reporting to a self-regulatory body constitutes an important safeguard for upholding the protection of fundamental rights as concerns the reporting obligations applicable to lawyers".

[84] See Chapter 2, par. 2.1, for a broader analysis and discussion on the FIU's receipt function and on cases where, besides the exceptions allowed by the Directive and examined in this paragraph, this function is affected by limitations or constraints related to indirect or multiple reporting.

It is important to underscore that filtering information out from STRs/SARs may adversely affect the FIUs' capacity to perform effective analysis on the suspicious activities detected. Even more so, of course, when the filtering goes as far as to allow the self-regulatory body to decide not to forward disclosures to the FIU based on own evaluations. It is not by chance that these forms of active interposition in the reporting procedure are not allowed by the Directive which, as said, while allowing for limited cases of indirect reporting, nonetheless requires that the end result of "fully" and "promptly" appraising the FIU is always achieved.

Lack of information in the disclosures forwarded to the FIU may hamper the analysis or require longer timeframes for understanding the case (by possibly acquiring the needed information through other sources on an ex-post basis). Possible cases where the filtering implies anonymisation, that is the omission of references to the reporting professionals, who has witnessed and verified the reported activities and may possess further elements, may even prevent the FIU from obtaining information from such professionals or otherwise put obstacles to the exercise of this necessary power.

Similar detrimental effects can be produced by these forms of filtering information out of STRs/SARs for certain categories of reporting entities on the FIUs' capacity to provide cooperation to foreign counterparts.

2.4 The reporting procedure: means and channels used

The use of dedicated IT means and procedures assisting the reporting and receiving process is considerably widespread across EU FIUs. However, it is somewhat surprising to learn from responses that in several cases the adoption of such IT means and procedure is relatively recent, with some FIUs still managing the transition from different, paper-based systems and implementing the recently introduced tools.

Some respondents indicate that well-established IT systems are in place since some time to manage incoming disclosures, equally filed electronically by reporting entities. These systems are in many cases web-based, thus allowing for direct and secure communication channels between the FIU and the reporting entities. In other instances, communications are assisted by secure e-mail tools. Encryption tools are also used, adding a further layer of security.

The following examples of IT reporting procedures, mentioned by respondents to the Survey, can be recalled:

- "obliged Entities report directly to the [FIU]" which uses "secured communication channel (…) for contacts with banks and financial institutions";
- "it is a requirement that STRs submitted according to the Money Laundering act are transmitted electronically to the FIU (via a dedicated website). This allows the data to be loaded and registered directly into the FIU's database";
- the reporting is "direct through dematerialized and secured process" or "the banks are connected with the FIU directly via VPN"; other respondents highlight that "STRs are mainly submitted electronically through the [FIU's] online portal" or through "encrypted emails";
- "the SARs shall be dispatched (…) in the form of a secure electronic message, and the [FIU] confirms the receipt of the SARs in the form of an electronic message sent to the reporting service provider";
- "STRs are reported directly to the [FIU] through the ad-hoc (…) procedure put in place for this

specific purpose; this connects directly, in real time, each obliged entity with the FIU". This procedure "allows for a secure and timely online transmission of the reports. The reports are sent electronically via Internet in an encrypted format and are automatically loaded into [the FIU's database] in a structured format, allowing to highlight the links between the subjects involved, the suspicious transactions and the financial accounts, automatically checking for the conformity of the incoming reports".

Interestingly, an FIU has informed that ad-hoc data transfer mechanisms are made available to assist reporting entities which file high volumes of disclosures.

More specifically, this respondent indicates that, while "most reporters use (…) a secure web-based reporting mechanism that, upon registering, can be used by anyone with internet access", "the main reporters use a bulk data transfer mechanism which is more appropriate for their volumes. For this, the [FIU] provides 'Public Key Infrastructure' encryption certificates which allow high volume reporters to submit encrypted files directly onto the SARs database".

The use of structured IT systems by FIUs for receiving and managing incoming disclosures entail that reporting entities are equally required to make use of IT tools and procedures to compile and forward STRs/SARs and to ensure appropriate connections with the FIU's systems.

As mentioned, some FIUs highlight that they are in the process of implementing IT systems for managing incoming disclosures or are still planning to transition to such systems whereas, in the meantime, different and more traditional tools continue to be used, in some cases based on paper transmission and manual upload of information into the FIU's own systems.

For example, a respondent to the Survey informs that it "currently receives up to 65% of all STRs electronically" from major institutions, whilst "the remainder is received in a paper-based format and manually entered onto the database". The same FIU also points out that it "is currently examining a web-based submission format for all STRs". Another respondent indicates that it "receives STRs transmitted by obliged entities automatically" and that "the additional information is added by manual work".

In many cases, FIUs do not develop and put in place own IT proprietary systems for receiving and managing incoming disclosures. They rather prefer to purchase from external providers IT packages which can be adapted and tailored to fit into the FIU's structure and procedures and suit to its operational needs. This option may be driven by considerations about costs but may also depend on the absence, within the FIU's organization, of dedicated IT structures, adequately staffed and budgeted, which can build and maintain dedicated own IT systems and procedures. Many respondents, in fact, inform that they are using, or are planning to use, the "GoAML" system developed by the United Nations specifically to assist FIUs in their receiving and case-management tasks.

Cases where FIUs implement external IT packages and tools in support of their own functions, while certainly efficient and advantageous under several important respects, should be considered in light of potential issues deriving from the reliance on support from third parties for functioning, assistance and maintenance, with possible impacts on effectiveness, security and independent operations, also depending on the terms regulating the levels of services.

One of the advantages of using electronic systems for reporting and receiving disclosures derives from the possibility of connection or integration between the IT transmission channels and the FIUs' internal case-management analysis system. Structured IT reporting formats, for example,

facilitates the upload of all relevant information into the FIU's own system and the cross-matching of data with available databases.

Due to the incomplete implementation of IT reporting and receiving tools by EU FIUs, in several cases STRs/SARs can still be filed through different channels: paper-based systems continue to be allowed in this context for producing and transmitting disclosures. While responses to the Survey show that these systems are only used to a limited extent, pending the transition to IT-based solutions, producing, transmitting and processing paper-based disclosures raise concerns about the security and confidentiality of information, as well as about the efficiency of the reporting procedure, possibly affecting the timeliness and effectiveness of analytical activities (and of FIU-to-FIU cooperation).

2.5 Timeframes for reporting suspicions

STRs/SARs must be reported "promptly" by obliged entities upon the detection of suspicions, as stated in article 33 of the Directive. While a specific timeframe is not set out, as this can reasonably depend on local circumstances (related to, for example, the reporting procedure and the information content of the disclosures), the Directive also foresees that disclosures should be filed before the execution of the transactions reported as suspicious, where this is possible, and that the reporting entities should refrain from executing these transactions while the reporting process is ongoing (until receiving instructions from the FIU, specifically as regards the consent to proceed or the decision to issue a postponement order, as also foreseen by the Directive in article 32(7)).

Based on the responses received, these provisions set out by the Directive appear to be transposed into domestic laws by Member States, in general, with little additional details spelt out, particularly as regards the amount of time allowed to file the disclosure after the suspicion has arisen and the cases where the reported transactions can be executed as refraining from their completion during the reporting procedure is considered not possible. In several cases, national provisions simply reiterate that STRs/SARs have to be reported "immediately" or "promptly", as soon as there is a suspicion that money laundering or terrorist financing activities may be carried out or attempted. Whenever these activities have not been executed, the obligation to report is accompanied by a duty to refrain from execution.

Many respondents to the Survey indicate that, while no specific timeframe is set out, reports must be filed "immediately", "unhesitatingly", "as soon as practicable" or "without delay". These responses also confirm that the disclosures should be filed before the transaction is executed, "if possible", or otherwise immediately afterwards.

In other cases, indications are given to reporting entities as to a timeframe within which disclosures must be filed after suspicions are detected. These indications normally refer to a maximum delay which should not be exceeded in any case. Still, the main obligation remains to file the reports immediately, that is within the shortest time possible and without waiting for the set maximum deadline to expire.

Responses show that, in cases where a maximum delay for filing STRs/SARs following the detection of a suspicion is provided for, this ranges from less than two hours to five working days. For example, a respondent highlights that "reporting entities are required to submit STRs [to the FIU] as soon as is reasonably practicable but not later than five working days from when the knowledge or suspicion first arose".

In cases of emergency or urgency, it is often explicitly prescribed that the disclosures should be filed immediately, regardless of the possible maximum timeframe allowed by the law for ordinary cases.

As regards the implementation of the obligation to file reports promptly, and the timeframes for these reports to reach the FIU after the detection of suspicions, responses do not carry detailed or comprehensive information.

On this point, though, a respondent informs that, against the obligation in place in its Country to send disclosures "without delay" upon the detection of suspicions, the delay between the moment when the transaction is performed and the moment when the STR is filed due to the detection of suspicions is decreasing: "In 2014, 55% of the reports were submitted within one month from the transaction (44% in 2013) and 71% within two months (65% in 2013)".

Importantly, the timeliness of the disclosures, on which the FIUs' capacity to take quick action depends crucially, may be affected by the use that is still done of paper-based reporting procedures (see previous paragraph), as these procedures require longer times for compiling, transmitting and processing STRs/SARs information.

In fact, a respondent specifically indicates that "the timeframe for receiving [disclosures] is immediately (…) and one-two days on paper".

2.6 Conclusions on disclosures of suspicious activities

As regards particularly the content of STRs/SARs, responses seem to suggest that, while there are commonalities, especially as regards the structure, significant differences exist with regard to the content, that is the type of contextual information, the level of details, the depth of records (especially those concerning financial transactions and background). These differences in the obligation for reporting entities to disclose suspicions affect the features of the analytical functions of the FIU. At the same time, conversely, it is based on the nature of the analysis which is entrusted to the local FIU that the prerequisites, structure and information content of STRs/SARs are shaped or fine-tuned in each Member State[85].

In fact, neither the FIUs' "analysis" function (as already discussed in this report) nor the "suspicious transactions" reporting obligation are defined or described in details in the EU AML/CFT framework (international standards or guidance, for example from the FATF or from the Egmont Group, are also lacking on these matters). This seems to determine a situations where the two influence each other in a feedback "loop" that has to be entirely managed and shaped at the domestic level within each Member State. As a result, the obligations to report and the analytical functions, while closely related nationally and strictly mutually depending in each local system, tend to differ significantly across the EU, resulting in a scenario which is considerably varied and fragmented along national lines.

While differences in the duty to report suspicions by obliged entities and in FIUs' functions are clearly justified and necessary to a certain extent to reflect local circumstances and peculiarities[86],

[85] E.g. through the issuance of indications to identify "suspicions" or "grounds to suspect" or by means of pre-defined, and more or less detailed, templates provided to reporting entities for preparing and filing their disclosures: see the information and considerations in the following paragraphs.

[86] For example, disclosures may well vary depending on the types of obliged entities and the exposure to different threats; the analytical activities, on turn, may change in function of the volumes of disclosures and on the expected use by police or judicial bodies after dissemination.

they can also have a significant adverse impact on several aspects of the compliance with AML/CFT obligations and of the FIUs' activities and cooperation. The following elements and considerations seem to stand out particularly in this regard.

- Differences in STR/SAR/UTR obligations may increase difficulties in compliance by obliged entities that have a cross-border presence or operations and a related need to apply uniform approaches to assess risks and identify and report suspicions at the firm or group level.

- The STR/SAR/UTR structure and content determine (or directly influence) the FIU's capacity to carry out analysis and also the nature of this analysis. As discussed, the "focus" and content of the disclosures depend on (and, at the same time, determine) whether the FIU's scrutiny is more geared towards a financial analysis or points instead to law enforcement-oriented actions, thus exacerbating existing "deviations" from a common approach to "analysis" as an FIU core function[87].

- Differences in disclosures at the national level also affect FIU-to-FIU cooperation, in several ways. Due to different information and data sets available to FIUs, the capacity to share is uneven and the likelihood of receiving useful information is reduced. Also, faced with the obligation to forward cross-border disclosures (see article 53(1) of the Directive), FIUs will exchange reports that are different under several respects (as they reflect national peculiarities) and may not even be "recognized" or usable by the recipient counterparts to the detriment of the capacity to identify and tackle potential cross-border money laundering or terrorist financing activities. The capacity to develop "joint analyses", as also foreseen by the Directive (article 51) may also be affected, both because FIUs' analysis is triggered by disclosures that differ substantially at the national level and because the information available and the approaches to their consideration and analysis vary to a significant extent (ranging between financial analysis and police action).

To facilitate obliged entities' compliance with the reporting obligations and allow for a more effective functioning of FIUs' analytical activities and cooperation, it may be worth considering: a) a more focused exercise on the content of STRs/SARs and on the effects of their differences; b) the setting out of common elements underpinning the disclosure of suspicious activities and its structure and content, through legislation or guidance at the EU level. This could be achieved, for example, by defining a common template for STRs/SARs to be used as a uniform basis throughout the EU.

The setting up of a common framework for the information structure of STRs/SARs would also facilitate compliance by obliged entities that have a cross-border dimension, both by allowing to report suspicions uniformly across multiple countries of operations and by improving the flows of information at the firm or group level. FIU-to-FIU cooperation would equally be facilitated as the set of information initially received, and available for the exchange, would be common across Member States in its essential features.

Importantly, the existence of heterogeneous contents and formats is also critical to a direct sharing of STRs with a cross-border dimension, as provided under Article 53(1) of the fourth Directive. In fact, a cross-border STR forwarded to the competent FIU may not be "recognized" as such by the recipient, due to a different notion or format being in place in its national framework. This can lead to failures of this important form of cooperation.

[87] See Chapter 5.

3. Other domestic disclosures received by FIUs: nature and content of threshold-based disclosures

In addition to disclosures concerning activities suspected of being linked to money laundering or terrorist financing, the Directive also envisages that FIUs receive "other information relevant to money laundering, associated predicate offences or terrorist financing" (article 32(3)). Recital 37 clarifies that information reported to FIUs, besides STRs/SARs, "could also include threshold-based information". Threshold-based disclosures are referred to particular types of transactions (such as for example, cash deposits or withdrawals or transfers of funds) and become due whenever a specified quantitative threshold is reached or exceeded, regardless of the suspicious nature of the underlying activities[88].

A particular type of disclosure based on objective features associated with certain operations and specified amounts is foreseen as mandatory for Member States by Regulation (EC) 1889/2005 "on controls on cash entering or leaving the Community": under article 3, "any natural person entering or leaving the Community and carrying cash of a value of 10.000 euro or more shall declare that sum to the competent authorities of the relevant Member States". While these declarations are ordinarily filed to customs agencies, they have to be "made available" to the FIU of the interested Country (article 5(1) of the Regulation).

In addition to these mandatory disclosures concerning the physical cross-border transportation of cash, responses show that only a minority of EU FIUs receive threshold-based reports. Moreover, the types of the disclosures received by this minority of FIUs are similar to each other, as they seem to converge into few common models.

The majority of objective disclosures received by EU FIUs concern transactions in cash above specified thresholds, consisting in deposits or withdrawals. Based on responses, the scope of the entities required to report this information is in principle the same as that of the entities obliged to disclose STRs/SARs. It includes banks, payment service institutions, electronic money institutions, but also certain categories of non-financial businesses and professions (such as notaries and casinos). The amount of the threshold that triggers these cash disclosures ranges between 10.000 and 32.000 euro.

Other types of objective disclosures are related to fund transfers operations: two respondents indicate that they receive reports on transfers above 1.000 euro (or even for lower amounts in case a monthly threshold of 2.000 is exceeded by cumulating multiple transactions) and above 30.000 euro, respectively. In this latter case, the duty to disclose only applies to transfers "related to countries where greater risks for ML/TF exist".

Other respondents highlight that they receive reports from other domestic competent authorities, concerning potential cases of money laundering or terrorist financing or information which is considered otherwise useful for the FIU's analysis. For example, respondents have referred to reports sent to the FIU by police agencies, the customs, intelligence bodies, supervisors and tax authorities. While these types of disclosures are certainly relevant and useful in support of the FIU's analysis, they seem to stem from forms of domestic inter-agency cooperation, rather than consisting in genuine threshold-based reports under the meaning of the fourth Directive.

[88] Conversely, the obligation to report STRs/SARs applies "regardless of the amount involved", as explicitly recalled by article 33(1)(a) of the Directive.

In few other cases, respondents to the Survey have referred to further types of disclosures that they receive in accordance with their domestic legal framework, in support of analytical activities.

For example, an FIU informs that it receives disclosures concerning: cases where obliged entities refuse customers because the CDD procedure cannot be completed, including information on the funds that are returned to the customers; transactions in gold exceeding a threshold of 12.500 euro; "aggregated data" sent by financial intermediaries and concerning their activities "for the purpose of performing targeted analyses [on] possible money laundering or terrorist financing contingencies in certain geographical areas".

Another respondent refer to "unusual transactions (threshold transactions) which must be reported to the FIU" based on "more than 20 different indicators for various types of reporting entities"[89].

The following table provides an overview on suspicious-based and threshold-based disclosures received by, or otherwise available to, EU FIUs.

[89] See Paragrah 2 on the nature of Unusual Transaction Reports and differences between those and STRs/SARs.

FIU	Suspicion-based disclosures	Threshold-based disclosures
Austria	SARs	Physical transportation of cash
Belgium	STRs	Physical transportation of cash Others*
Bulgaria	STRs	Cash Transaction Reports > € 15.000 Physical transportation of cash
Croatia	STRs	Cash Transaction Reports > HRK 200.000 (about € 26.500) Physical transportation of cash
Cyprus	SARs/STRs	Physical transportation of cash
Czech Republic	STRs	Physical transportation of cash
Denmark	STRs	Physical transportation of cash
Estonia	STRs	Cash Transaction Reports > € 32.000 Physical transportation of cash
Finland	STRs	Physical transportation of cash
France	STRs	Cash transfer operations > € 1.000 per operations or > € 2.000 cumulated in a month Cash deposit or withdrawal > € 10.000 per operations or cumulated in a month Physical transportation of cash
Germany	STRs	Physical transportation of cash
Greece	STRs	Physical transportation of cash
Hungary	SARs	Physical transportation of cash
Ireland	STRs	Physical transportation of cash
Italy	STRs	Physical transportation of cash Others**
Latvia	UTRs	Physical transportation of cash
Lithuania	STRs	Cash Transaction Reports ≥ € 15.000 Physical transportation of cash
Luxembourg	STRs	Physical transportation of cash
Malta	STRs	Physical transportation of cash
Netherlands	UTRs	Cash Transaction Reports > € 15.000 Money Transfers > € 2.000 Physical transportation of cash
Poland	STRs	Physical transportation of cash Transactions > € 15.000 (> 1.000 for casinos)***
Portugal	STRs	Physical transportation of cash
Romania	STRs	Cash Transaction Reports > € 15.000 External transfers > € 15.000 Physical transportation of cash
Slovak Republic	UTRs	Physical transportation of cash
Slovenia	STRs	Cash Transaction Reports > € 30.000 Wire transfers > € 30.000 Transfers of cash > € 10.000 Physical transportation of cash
Spain	STRs	Cash Transaction Reports Physical transportation of cash
Sweden	STRs	Physical transportation of cash
United Kingdom	SARs	Physical transportation of cash

Table on suspicious-based and threshold-based disclosures

* Disclosures from Notaries and Casinos
** Aggregated data > € 12.500 and Transactions in gold > € 12.500
*** Transactions registered by obliged entities and reported to the FIU on a monthly basis

3.1 Reporting procedures and timeframe for threshold-based disclosures

In line with existing provisions in Regulation 1889/2005, declarations on the physical cross-border transportation of cash are filed to the national customs agencies, which gather centrally all received data. Based on responses, no cases have been reported where it is the FIU that receives directly these declarations[90]. This data, again in accordance with Regulation 1889/2005, is then made available to the FIU by the receiving agency. Responses show that FIUs do not normally have direct access to the information received and held by customs agencies. Rather, they receive such information, in turn, through a sort of additional disclosure by these agencies.

This disclosure is carried out (normally by transmitting or making available bulk data, that is not each individual declaration the moment it is filed by the obliged individual) through various means. Although responses are not sufficiently detailed on this point[91], it appears that the majority of the EU FIUs receive this data systematically from the customs authorities, although technical modalities and practical arrangement may differ and the timeframe within which the FIU is appraised may vary as well. Generally, customs agencies either forward the declarations or provide the FIU with their information content.

A respondent to the Survey indicates in this regard that "both the declarations and information concerning observed instances of non-compliance must be forwarded to the FIU by the [Customs] and are entered into the [FIU's] database". Other respondents also report systems of direct forwarding of declarations (or of their content) to the FIU by the Customs.

This forwarding can also take place through automatic means.

A respondent flags that "information about cross-border cash declarations, submitted to the Customs officers, is entered into the cash-declarations data gathering and processing system and automatically provided to the FIU".

In other cases, Customs provide the FIU with information on cash declarations through more indirect ways, through ad-hoc communications based on certain features, modalities and timeframes.

For example, a respondent has informed that "cash declarations are received [from the Customs] in a structured format, excel, on a monthly basis". In another case, the procedure for the provision of such information "is determined jointly by the State Agency for National Security and by the Minister of Finance".

In lack of forms of direct access by the FIU to the database gathering and storing the information received by the Customs through declarations of cross-border transportations of cash, it is important that the mechanisms in place to forward or share this information with the FIU allow for the necessary rapidity and security. An excessively long time-lag between the cash transportation (or the declaration) and the transmission of the related information to the FIU may deprive the latter of data useful to conduct analysis effectively. Timely information on activities involving cash (or bearer instruments) may be particularly relevant in terrorist financing-related analyses. While periodic transmission of data packages in structured formats may be efficient but less timely,

[90] It is worth recalling that the Regulation 1889/2005 generally refers to "competent authorities" as the recipient of such declarations and, therefore, does not rule out the possibility that FIUs are designated for this purpose.

[91] A dedicated survey could be considered on technical means, procedurs and timeframes for the FIUs' access to information on cash cross-border physical transportation held by customs agencies.

automatic forms of sharing or transmitting declarations, or their content, may be more conducive to prompt consideration by the FIU (and equally efficient).

For what concerns the other threshold-based disclosures that EU FIUs receive in addition to STRs/SARs and declarations on cross-border transportations of cash, responses show that these are in all cases directly received by the FIUs themselves, in most instances through the same channels and modalities used for the transmission of STRs/SARs. As a consequence, IT systems are normally used for filing and receiving these disclosures, based in formats defining their structures and information contents.

Several respondents to the Survey confirm that threshold-based disclosures are received directly by the FIU through the same systems and channels used for STRs/SARs. It is also highlighted that the transmission is "dematerialised and secure" and "according to structured formats and through IT tools and procedures, which ensure rapidity and security".

Nonetheless, there are also cases where threshold-based disclosures are transmitted and received through more traditional, paper-based, formats and procedures, similarly, as seen in paragraph …, to what happens also for the disclosure and receipt of STRs/SARs.

A respondent has indicated that "reporting entities submit CTRs (…) in hard copy or using magnetic media or electronically using a template".

The timeframes foreseen for sending threshold-based disclosures vary considerably across Member States. In several cases, the deadline for the transmission is set based on the day when the transaction that triggers the reporting obligation is performed. Responses show that the available time span for the disclosure ranges from two working days to seven working days from the execution. In other cases, the disclosures are due on a monthly basis and are sent in bulk transmissions including information related to all transactions performed in the month of reference.

For example, a respondent flags that "threshold-based disclosures are ordinarily transmitted the month after that of the performance of the relevant transactions". Others adopt similar system: reports shall be forwarded to the FIU till the 5th day of the month which follows the previous month (in which the case has happened)".

As regards the receiving phase, this takes place "in real time" in those cases where the disclosures are compiled and transmitted through IT tools and the FIU avails itself of electronic procedures to process the information and upload it into its systems.

3.2 Conclusions on threshold-based disclosures

Threshold-based disclosures are foreseen by the Directive and domestic legislations as tools, additional to suspicious-based reports, aimed at assisting FIUs in their analyses by making information available on activities and transactions which, although not specifically linked to particular anomalies or suspicions, may be relevant for the identification of matches and correspondences with other transactions, as well as for the detection of overall phenomena or trends in particular sectors or through the use of particular tools or operations.

Given that, based on the responses, only a minority of EU FIUs receive threshold-based or objective disclosures (besides the mandatory declarations concerning the cross-border transportation of cash), the question can be asked of whether this tool should be implemented more broadly to expand the

scope of the information available to EU FIUs and consequently enhance their analytical capabilities.

For example, while recent experience has indicated that the consideration and analysis of fund transfers operations and remittances are critical for the early detection of terrorist financing activities and the identification of network of support to terrorism, only few Member States have introduced measures for the disclosure of transfers of funds as objective transactions. Moreover, these disclosures, where they are required, are in most cases only due for relatively high amounts (e.g. 30.000 euro), whereas terrorist financing may take place through much smaller transactions. According to responses to the Survey, in only one case, as highlighted above, a Member State has introduced an obligation to report transfers exceeding a more suitable threshold of 1.000 euro.

The consideration that in those Member States where threshold-based reports are foreseen by the law these reports are related to a particularly limited range of transactions (mostly, as discussed above, cash operations and transfers of funds) should also lead to further reflections on whether additional, more varied types of disclosures and information would be beneficial for FIUs to develop effective analysis and reinforce their capacity to identify suspected money laundering and terrorist financing activities across the multiple and differentiated sectors of the economy from which STRs/SARs also originate.

It is also necessary to underscore that respondents have not informed about plans currently being considered at the national level to introduce further disclosure obligations. Only one FIU mentions that "it is hoped that additional threshold-based disclosures will be introduced by future legislation in support of [the FIU's] analysis".

To address these concerns, the need for more detailed provisions or guidance at the EU level should be considered. Building on current provisions in the fourth Directive which, in line with the FATF Recommendations, mentions threshold-based disclosures as an additional tool, complementary to STRs/SARs, to provide the FIU with relevant information, specific types of objective reports could be explicitly set out as mandatory for Member States to implement domestically or, in alternative, as guidance to conform possible national measures to identified and tested models to which national practice could converge.

EU provisions or guidance could also be helpful to consolidate types of threshold-based disclosures that, based on the best practices developed by Member States and their FIUs, appear to be particularly useful in support of FIUs' analysis. Based on the results of the survey, as already highlighted, most common types of disclosures which could become models for all Member States are those related to transactions in cash and transfers of funds. As also highlighted, lower thresholds for such disclosures would seem appropriate, particularly to allow for a most effective capacity to detect terrorist financing-related activities.

Responses show that the timeframes for reporting threshold-based disclosures are different across Member States, as different are also the systems used and the criteria to set applicable deadlines. Understandably, there is generally not an obligation to disclose this information "promptly" or "immediately" upon execution of relevant transactions[92] and, similarly, there is not an obligation to refrain from executing the reported transactions. In fact, these are not related to suspicious money laundering or terrorist financing cases and are destined to be used by the FIU to support its analytical functions (and international cooperation activities as well).

[92] Although some responses refer to a duty for reporting entities to file objective disclosures "immediately".

Nonetheless, it is important that objective disclosures reach the FIU in a timely manner, for two quite obvious concurrent reasons: firstly, although not reported as suspicious, the underlying transactions may well become such in light of possible additional information available to the FIU, which could therefore need to act quickly upon them; secondly, information in objective disclosures may be directly relevant for ongoing analyses and, therefore, may have to be rapidly considered to better assess the case and determine the most appropriate follow up.

The use of structured templates and of electronic tools for compiling, transmitting and receiving threshold-based disclosures is also essential: on the one hand, to ensure that these can be rapidly and safely detected and transmitted by obliged entities; on the other hand, to allow the FIU to find correspondences with STRs/SARs or other available information and to make the received information available for analysis and international cooperation.

4. Access to "financial", "administrative" and "law enforcement" information. General aspects

Pursuant to Article 32(4) of the fourth Directive "Member States shall ensure that their FIUs 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".

In response to the direct question of whether the FIU has access to financial, administrative and law enforcement information that is required to fulfil its tasks properly, EU FIUs have understandably confirmed that this is the case. Nonetheless, several respondents have indicated that they see "space for improvement"[93].

Some respondents to the Survey have stressed the importance of having access to centralised databases of bank accounts and of beneficial ownership, recalling that these are in the process of being set up within their jurisdictions, in line with the fourth Directive.

However, the more targeted and granular assessment of responses provided to detailed questions on categories of information available has uncovered several areas of weakness, as well as significant differences across EU FIUs. These categories of data labelled as "financial", "administrative" and "law enforcement", are only generically identified in the Directive and not further described, thus leaving Member States with a considerable degree of discretion in determining the types of information which may be available to their respective FIUs. This, in turn, translates into significant differences in the range of information available to EU FIUs and, as consequence, in their capacity to carry out effective domestic analysis and develop effective cooperation with foreign counterparts.

As a way of example, some respondents have succinctly described the information sources they have available for analytical purposes. While the following paragraphs will be specifically dedicated to the access to bank account and beneficial ownership information, and to related differences and potential issues, the table below provides an overview, for some FIUs that have submitted more detailed elements in this regard, of the types of information available. This overview also shows how difficult and somewhat arbitrary, in lack of definitions or descriptions, it would be to draw distinctions among "financial", "administrative" and "law enforcement" categories of information.

[93] A respondent, though, has interestingly flagged that the scope of the information it has available could be improved , to better support its analysis and has put forward some examples of possible improvements: "Comparing (semi-automatically) the FIU information against information in other databases" and "automatic importing of tax information".

FRANCE	ITALY	UK
Tracfin has full access to the centralised bank accounts registry (FIchier des COmptes Bancaires et Assimilés – FICOBA). Article 1649A of the General Tax Code requires public administrations, establishments or bodies subject to supervision by the administrative authority and any persons that habitually receive or deposit transferable securities, certificates or cash to declare to the tax administration the opening, modification and closing of accounts of any kind. Tracfin can exercise its power to request additional information from: • reporting entities, • transportation (air, maritime, ground, rail) companies or tour operators (Article L. 561-26 of the monetary and financial code). Tracfin daily uses its own database, where any inward information is recorded and implemented. In addition, Tracfin can access, whether directly or indirectly through his custom and social security institution liaison officers to: • General and "reputation" Information databases (i.e. World-check, Dow Jones) • Business information databases (i.e. Trade and Company Register, …) • Custom, tax and social security protection databases Tracfin has indirect access to law enforcement databases through his liaison officers from the police and the gendarmerie and his liaison magistrates. Since late 2016, beginning 2017, Tracfin will get a direct access to these databases. Tracfin has the capacity to obtain directly additional information from any obliged entity, not only from the one having reported a suspicious transaction (Article L. 561-26 of the monetary and financial code).	UIF has access to various databases, internal and not, information at disposal of obliged entities and of other Authorities. In particular, UIF uses information provided by other Authorities (Bank of Italy, Consob, IVASS, Customs Agency) on the basis of MOUs; more in general, AML legislation establishes collaboration obligations between the FIU and relevant administrations, professional orders, sectoral supervisory authorities (…), judicial authority and investigation bodies. This information allows UIF to perform properly the analytic functions on suspicious cases. The same sources of information are available also for international exchanges with foreign counterparts. In particular, UIF has access to the following external sources: • online access to the information in the company's registry, relating to equity investments, the positions of management and the accounting data of the Italian companies; • online service "Orbis", with similar information on companies with foreign headquarters; • online services of data providers "World Check" and "Compliance Daily Control"; • the "Risk Central Database", managed by the Bank of Italy, which allows to verify the debts of reported subjects toward the entire Italian financial system; • the "Accounts and Deposits Database", managed by the Internal Revenue Service with information on accounts, both current and closed, and the transactions outside the accounts; • The Cross border Declarations Database, with information on physical transfers to/from abroad of cash or bearer valuables; • Target2, with information on wire transfers in the Euro area; • Archive of disciplinary decrees issued by the Ministry of Economy, real estate and mortgage data	• FIU-Database - Suspicious Activity Reports (SAR) - Always completed • Criminal records (convicted persons) and limited arrest records - On request • Vehicle register – if registration mark provided - Registered keeper • Address Information – if full subject details provided • Commercial database check only – possibly more information available via Interpol/ UK Police • Land/Property ownership records - Only if address provided and only registered proprietor • Company register (incl. officers) - On request • Directors, shareholders and members of companies (if declared) - On request • Outstanding court confiscation orders - On request • Confirmation of bank branch detail from sort code and account number - On request • Bank Account information - ILOR: UKFIU can only confirm bank details from sort code and account number • Transactions of clients of banks and other financial institutions – ILOR • Police reports of crime and operational reports - UK Police - via Interpol • Records of real Beneficial Owners - No B/O register currently in place • Border crossing by physical persons - If held - only available via Interpol • Register of physical persons (record of births, deaths and marriages) - UK Registrar's Office hold this data • Passport and visa details - UK Passport Office hold this data • Declared income and taxes paid - UK HM Revenue & Customs (HMRC) hold this data • Customs records - UK HM Revenue & Customs

	archive; • Tax registry, with data and information resulting from tax declarations and complaints and related verifications, as well as other data and information of possible fiscal relevance; • Central tax reports database (CEBIL) that contains ID tax data and tax declarations held by the tax agency; • Local administrators database (municipality, district and region).	(HMRC) hold this data • Export-import of goods - UK HM Revenue & Customs (HMRC) hold this data • Social security information (on physical persons) - Department of Work & Pensions (DWP) hold this data • Insurance licenses and compliance - Financial Conduct Authority (FCA) hold this data • Banking licenses and compliance - Financial Conduct Authority (FCA) hold this data • Stock market licenses and compliance - Financial Conduct Authority (FCA) hold this data • Money remittance licenses and compliance - UK HMRC (HMRC) hold this data • Gambling licenses and compliance - Gambling Commission hold this data

Table 8 – Examples of information accessible

4.1 General conclusions on FIUs' access to "financial", "administrative" and "law enforcement" information

As will be further discussed in the following paragraphs, responses confirm that EU FIUs have indeed access to considerably diversified sets of information that they variably (and somewhat arbitrarily, in lack of a definition or a common understanding of what these general categories include) label as "financial", "administrative" or "law enforcement". Beneath the issue of definition, lies an issue of scope. In several cases, the range of information available may be too limited to support the FIU's analytical functions adequately. Similarly, narrow availability of information domestically directly impacts the FIUs' capacity to provide effective cooperation to foreign counterparts.

Differences in information available (under the different labels of "financial", "administrative" and "law enforcement") may be particularly detrimental to smooth FIU-to-FIU cooperation for two complementary aspects. Due to the lack of a common notion about the nature and types of necessary information under each category, some FIUs have an insufficient range of information available and a correspondingly low capacity to provide assistance in response to requests from foreign counterparts.

Moreover, differences in the information available for the exchange (despite their common categorization as "financial", "administrative" or "law enforcement") entail discrepancies that can trigger the reciprocity condition and cause refusals to cooperate by those FIUs that, despite having the capacity to provide the requested information, are aware that they would not receive the same information in similar circumstances by the counterpart in question[94].

To avoid, or limit, these undesired adverse effects on FIUs' activities and cooperation, it may be worth considering to develop a common approach at the EU level on what should be a minimum scope of the information available to FIUs and what types of information should be included, as a common minimum, under the categories of "financial", "administrative" and "law enforcement". In this regard, a higher level of harmonisation seems particularly needed.

5. Financial and administrative information. Information on bank accounts through centralised databases or retrieval systems

The setting up of databases or other mechanisms allowing to retrieve information centrally on bank accounts held within banks established in the territories of Member States is not yet an obligation under the current fourth Directive. Nonetheless, pursuant to its Recital 57, "In accordance with union and national laws, Member States could consider putting in place system of banking registry or electronic data retrieval system which would provide FIUs with access to information on bank account without prejudice to judicial authorisation where applicable".

An obligation to set up such national registers or retrieval systems is now foreseen in the Proposal for a directive issued by the European Commission to modify the fourth Directive in selected matters. The "Action Plan to strengthen the fight against terrorist financing", issued by the Commission in February 2016, in fact, acknowledges that the capacity to identify whether a subject holds an account, and where this account is maintained, represents an essential component of the

[94] See Chapter 6 for a more specific analysis of the implications on FIUs' cooperation deriving from the insufficient and non-uniform range of information available to EU FIUs.

FIUs' capacity to carry out effective analysis to prevent and detect terrorist financing networks and activities (as well as, of course, money laundering operations).

The majority of respondents have indicated that they can have access to information allowing the identification in a timely manner of whether a natural or legal person holds or controls accounts within banks established in their respective territories. However, responses show that this capacity is only in some cases based on the availability of central registers with information on bank accounts or of other centralised systems for retrieving this information.

Such registers or systems are reported to be in place in 11 Member States, with their respective FIUs having access to them in support of their analyses[95]. Two respondents explicitly inform that appropriate regulatory reforms are underway and centralised bank accounts databases are expected to be set up shortly in their jurisdictions (similar developments may be ongoing also in other EU Countries).

Existing arrangements differ considerably across Member States as to the authority in charge of maintaining the central database or system, the nature of such database or system, the information that can be obtained. In one case, the centralised database of account holders has been set up within the FIU itself. In other Member States, it is held by other authorities such as tax administrations or the Ministry of Finance. In one case, it is reported that the FIU can have indirect access to a centralised database held by the Central Bank.

For example, a respondent to the Survey has indicated that "the Tax Authorities have information about all [national] bank accounts held at the end of every calendar year by individuals and companies liable to pay tax (…). This information is based on the banking sector's mandatory reporting of account information to the tax authorities. This information is directly available to the FIU upon request".

Similarly, other FIUs have informed that they have access to "the accounts and deposits database, managed by the [national] Internal Revenue Service" or that they receive information on bank accounts "by online access to State Tax Inspectorate data".

In other Member States, centralised registers with information on bank accounts are held by specialised agencies of a public nature or publicly owned, providing IT services.

In this respect, responses refer e.g. to bank accounts information held in a "Single Registry of Bank Accounts operated by (…) a State-owned agency established by a separate law". Another respondent informs that it has access to information on whether natural or legal persons hold or controls accounts "through the registry of bank accounts" based on an "online application developed by" a specialised IT agency within the Ministry of Finance.

The vast majority of respondents that report the existence of mechanisms to obtain centrally information on bank accounts held in their territories refer to ad-hoc databases set up specifically for this purpose (these databases may not be used exclusively by the FIU for AML/CFT activities and may be available for pursuing other activities as well, notably tax investigations). In fact, retrieval systems not based on centrally stored information, although they are equally foreseen as

[95] See also Annex 7 to the Euroepean Commission's Impact Assessment of proposals to amend theAMLD, with an anonymised overview of the current situation in the 16 Member States that have or are in the process of putting in place automated mechanisms that enable them to identify holders of bank and payment accounts (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2016:0223:FIN%20).

viable options in Recital 57 of the fourth Directive and in the Proposal for a new directive issued in July 2016, do not seem particularly pursued by Member States. Nonetheless, a respondent to the Survey has indicated that a different approach is followed in its Country to obtain centralised information on bank accounts.

In this case, the information is obtained "from credit reference agencies". While "this is not a central bank account register", the respondent is "satisfied that we can conduct checks via credit reference agencies to confirm" the existence of accounts.

As regards the information content that FIUs can extract from the consultation of available databases or mechanisms on bank accounts, responses show that this includes essential information on accounts and other banking relationships, such as the identity of the holder, the dates of opening or termination, the type of the account or relationship.

A respondent to the Survey flags that "the information that can be accessed is the 'PIN' (Personal Identification Number) and the name of the natural or legal persons, the account number, the date when the account was opened and closed, and other related information". Similarly, in another case the obtainable information includes the "bank account number, date of opening/closing of the account, currency; bank code; bank name; type of account".

Another FIU flags, more amply, that the centralised register "provides verification on the existence of all accounts, both ongoing and closed, and the transactions outside the accounts concerning the enquired subject inside the entire [national] financial system"; the database includes "ID data on holder of business relationships at banks/financial institutions, the list of business relationships (such as bank accounts, guarantees, loans, debit and credit cards, occasional transactions above thresholds), data of their opening/closure, indications on the existence of co-holders and subjects delegated to operate".

Based on responses, it appears that information on beneficial owners of bank accounts is not gathered or made available for consultation, despite this being an essential element of customer due diligence procedures applied for the opening of banking and financial relationships, with the relevant data being collected and kept up to date by banks. The possible lack of information on beneficial ownership represents a significant limitation to the completeness and usefulness of centralised bank accounts registers or mechanisms for FIUs' analysis.

The availability of centralised databases allows most of the times the FIU to have a direct and immediate access to information on bank accounts. This access is normally subject to authentication and verification procedures, by the organisation holding the register, and carried out ensuring adequate standards of confidentiality and security for the information obtained.

On this point, responses confirm that registers are available for online access "without the need to send written request" and by providing an appropriate "identification code" or "using digital signature authentication". A respondent informs, more specifically, that it has "online direct access on the basis of a MoU signed with the Revenue Agency"; the "access by authorised personnel is direct through authentication on the Agency's website. Queries are conducted under a full secrecy regime and under very tight security and protection conditions".

Direct online access allows the FIU to obtain information immediately, upon execution of the electronic query. While several respondents confirm that this is the case, few others indicate that information from central registers can be obtained after some delay. Timeframes can range from 24 hours to one month, also "depending on the nature and complexity of the request".

It can be observed, on this point, that the setting up of centralised electronic databases or mechanisms gathering information on bank accounts should facilitate the prompt extraction of data and that delays of days or even weeks would be hardly consistent with a requirement for FIUs to be able to identify whether natural or legal persons hold or control accounts "in a timely manner". The more so, as such searches may need to be performed under urgency conditions, particularly in cases where the FIU is tracing potential terrorist financiers or terrorist-related assets that should be made subject to immediate freezing restraints.

5.1 Other means of accessing information on bank accounts

While, as said, only eleven respondents to the Survey have indicated that centralised registers or mechanisms are in place in their Countries allowing to obtain information on bank accounts, several other FIUs (nine) have informed that, despite the absence of such databases, they can have access to information allowing the identification in a timely manner of whether natural or legal persons hold or control accounts.

In some cases, respondents flag that, when a bank account and its holder have to be found and identified in the financial system, "a request for information is sent to every bank". While this approach is likely to produce more results in countries with relatively smaller financial systems, it certainly does not seem to provide sufficient guarantees as to the FIU's capacity to obtain information in a timely manner and under appropriate confidentiality and security conditions.

An FIU informs that, when a bank account has to be identified, it "sends a written request to the banking supervisory authority". While also in this case timeliness and confidentiality may not be fully guaranteed, it is not clear how the supervisor obtains the information on behalf of the FIU (other than by interrogating the banks established in the national territory).

Responses on this point, in any event, seem to suggest that, in lack of centralised means for retrieving information on bank accounts, this information can only be obtained by FIUs by approaching individual banks, either directly, based on general information powers available for the analysis, or through another competent authority such as the sectoral supervisor.

Based on these information powers, FIUs can certainly obtain information on bank accounts and their holders and beneficial owners but, as such powers are exercised vis-à-vis determined banks, accounts or individuals, they can hardly be used to identify whether, and within what bank, a natural or legal person holds or control accounts in the first place. In other words, the exercise of powers to obtain information from a bank requires that the bank where the account of interest is held has already been identified; but this is precisely the objective which is allegedly pursued through the use of such powers.

A respondent, for example, in describing how bank accounts can be identified, underscores that "while there is no centralised accounts database, the legislation requires credit institutions/financial institutions to have systems in place to enable it to respond fully and promptly to enquiries from [the FIU] as to whether it has held a business relationship with a named person within the last 6 years and the nature of that relationship".

Similarly, it is remarked by another respondent that "the FIU can obtain all kinds of information" from reporting entities, including "information if a person is holding a certain account", and that this can be done "by contacting the respective reporting entity directly" as "there is no access to centralised bank data". Other respondents also point out that, although there is not a centralised

database with bank account information, "the FIU has the legal power to request and obtain information and/or documents with regards to the existence of a business relation and its nature and/or the beneficiaries of bank accounts and the balances of bank accounts".

Clearly, the power to obtain information from individual banks is particularly important for the FIU to retrieve data on accounts, their holders and beneficial owners, and the activities performed through them. However, this can only be done in cases where the banks that should be approached, as the accounts of interest are held within them, are already known. In cases where this objective is pursued by sending requests to all banks established in the territory, the considerations developed above on timeliness, effectiveness and confidentiality should be recalled again.

The capacity to approach individual banks and obtain information on specified accounts, therefore, does not solve the issue of how FIUs, when they do not know where individuals or entities hold their assets, can determine whether these individuals or entities hold accounts in their jurisdictions and, if that is the case, in what banks these accounts are maintained. Only after the questions are responded of "whether" accounts exist and, if yes, "where" they are held, can then the FIU effectively exercise its information powers to approach the identified banks with targeted requests for information on what are the features of the accounts and how they have been used, as needed for its analytical purposes.

5.2 Conclusions on FIUs' capacity to determine the existence of bank accounts

Responses received on this point show that only in few cases centralised registers or mechanisms have been set up in EU Member States allowing FIUs to obtain timely information on whether and where natural or legal persons hold accounts in banks established in their territories. While there is currently no obligation in this respect within the EU, there are strong indications that this is an important tool in support of FIUs' analyses on money laundering and terrorist financing (and, more broadly, for financial investigations in these matters by all competent authorities).

Importantly, in Countries where centralised databases or mechanisms exist to retrieve information on bank accounts, these have been set up based on different arrangements, particularly as regards the authorities where they are located, the information content and the access procedures. This may have implications on security and confidentiality and, as discussed previously, also on timeliness of access.

Outside of the few cases where centralised databases or mechanisms are in place, EU FIUs do not seem to have effective capacities to obtain through other means information on whether and where specified bank accounts are held by certain individuals or entities within their jurisdictions. In fact, the exercise of ordinary information powers available in support of the analytical functions vis-à-vis particular banks, as indicated by several respondents that do not have access to central registers or mechanisms, do not seem sufficient for this purpose.

Besides limiting domestic analyses and intelligence, the lack of capacity to obtain this information has also an impact on FIU-to-FIU cooperation. In this respect, while the reciprocity condition might prevent FIUs that can avail themselves of national bank accounts' databases from providing this information to foreign counterparts that cannot, the identification of bank accounts held domestically cannot in most cases be complemented with the identification of accounts held by the same subjects in other Member States.

This information would clearly be particularly important both for domestic analysis and for the development of further cooperation between the interested FIUs on potential illegal activities of a

cross-border nature carried out through bank accounts and assets held in multiple countries. The same information would also facilitate consistent, comprehensive and timely application of freezing measures across different Member States, pursuant to relevant Council Regulations introducing financial sanctions, and the effective performance of controls aimed at verifying implementation of these Regulations and compliance by financial institutions.

6. Information on the identification of assets

Recital 57 of the Directive, besides referring to "banking registers or electronic data retrieval systems" for locating bank accounts, also encourages Member States to consider setting up a "mechanism to ensure that competent authorities have procedures in place to identify assets without prior notification to the owner". No indication is provided on the types of assets, different from those held in bank accounts, that competent authorities should be able to identify. It is reasonable to assume that this scope could include other financial assets, such as securities or insurance policies, and non-financial assets, such as real estate properties. Although this is not specifically mentioned in Recital 57, the availability of information on assets would greatly benefit, in terms of completeness and rapidity, from the existence of centralised registers or data retrieval mechanisms.

The vast majority of respondents to the Survey have indicated that they can have access to information allowing the identification of assets. In some cases, reference is made to the FIU's capacity to obtain information from obliged entities, or perform enquiries based on available information powers, similarly to the responses discussed in the previous paragraph as regards bank accounts.

Some respondents recall their capacity to obtain information on insurance policies from insurance companies: "The FIU is empowered to request any information from any reporting entities, including life insurance companies and the life insurance policies they manage".

These responses are similar to those mentioned in the previous paragraph, on the FIUs' capacity to have access to information on bank accounts by approaching individual financial institutions. While this is certainly helpful in obtaining detailed information on specified individuals or assets, these have to be known in advance to the FIU in order for it to properly address targeted queries. The information on "whether" certain individuals or entities hold assets within the country, and "where" these assets are held, as essential to start the analysis, cannot be easily (or timely and confidentially) obtained by asking all obliged entities.

In other, more numerous cases, respondents provide feedback on how they can obtain information on assets (mostly, of a non-financial nature) by means of centralised databases they have access to. Most common types of accessible information concern real estate. Several respondents to the Survey inform that they have direct access to centralised land registries, generally by electronic means. The information which is most commonly obtained by FIUs on real estate assets includes the current ownership, value, past transfers of property, location. However, the types of databases, their contents and the access conditions vary considerably from Country to Country.

An FIU indicates that it can access two databases: information on "sales/purchases of real estates or payment of the tax on real estate" is available "through the Tax Administration Information System"; information "on the persons owning the real estate and on the history of the transactions" is available from the "Land Registry Court" (both databases can be consulted online). Another respondent also informs that it can access "two real estate-related registers": "One is land register searchable by land number where are all data about property (ownership, claims, history of ownership, etc.) and cadastral register, searchable also by owners name, where are more technical

data about the property (current ownership, value, etc.)".

In some cases, access to real estate information by the FIU is not direct and may be subject to conditions or longer timeframes.

For example, a respondent highlights that is has "direct electronic access to Register of Real Estate", where "only basic information is available (if the person or the entity possesses real estate and location of the real estate)"; a "written request has to be made to a competent institution for collection of further details". Other respondents flag that they can access real estate or land registers "through a third party" (one of these respondents specifies that this happens "with no need for motivation").

Besides registers on bank accounts and on real estate, some FIUs recall that they can have access to other databases with centralised information on assets held in their countries and their owners. In several cases, registers on vehicles are available; less frequent is the availability of databases with information on shareholdings in companies (although access to companies or business registers, with information on directors and shareholders, may be more common and widespread: see also the following paragraph). Interestingly, one respondent has indicated that it has access (online) to "tax assessments of income".

6.1 Conclusions on access to information on the identification of assets

The survey shows that EU FIUs have significantly different capacities and tools to obtain information allowing the identification of assets held in their territories. While some rely on the power to obtain information from obliged entities, this does not seem to provide an effective and efficient means to identify assets whose existence and location is not previously known.

Only a portion of EU FIUs seem to have access to centralised registers or databases for this purpose. Even there, together with significant commonalities (e.g. as regards the relatively widespread capacity to access information on real estate through direct online mechanisms), differences exist in the types of registers or databases available, in the scope of the information that can be obtained and in the access procedures (which inevitably impacts on the timeframe for obtaining the information).

7. Information on legal and beneficial ownership. Central databases

Along the lines of the revised FATF standards, the fourth Directive requires Member States to ensure that information on beneficial ownership of corporate entities and trusts, in addition to data on legal ownership, be collected and held and made available to competent authorities and FIUs (as well as to obliged entities for discharging their customer due diligence obligations). The Directive, while obliging corporate entities and trustees to maintain and keep up to date the information on their respective beneficial ownership, also requires each Member State to set up a "central register" ("for example a commercial register, companies register (…) or a public register") where the information on beneficial owners should be held and made available for access by the subjects entitled (see article 30 and 31).

Differently from the FATF standards, which maintains a certain level of flexibility as to the means through which information on beneficial ownership should be made available to FIUs and

competent authorities[96], the Directive requires that all beneficial ownership information should be stored in central national databases that are established as a necessary means to achieve the purpose of allowing FIUs (and other competent authorities) to retrieve reliable and fast information on possible beneficial ownership positions held by individuals, without knowing in advance whether such individuals actually are beneficial owners and in what companies, legal entities or trust arrangements.

It is important to recall that, in accordance with the definition of "beneficial owner" (article 3(6) of the Directive), while in many cases beneficial and legal ownership may be conjoined, they may equally well differ and the latter should always be identified and determined separately and autonomously, with the relevant information being acquired and kept up to date in a central register.

As regards the capacity of EU FIUs to access information on beneficial ownership, responses show that only few of them can obtain such information and that the obligation (for Member States) to set up central registers for this purpose has not been fulfilled yet. On the other hand, companies registers with information on legal entities (including their legal ownership) appear to be widespread and generally available to EU FIUs.

In fact, responses suggest that the vast majority of EU FIUs can have access to central registers with information on companies and other entities set up or established in their territories (but four respondents indicate that they do not have access to such information). However, in all reported cases where central companies registers are set up and available for the FIUs' enquiries, information on beneficial ownership is not specifically or systematically collected and kept up to date. In this respect, reference is often made in responses to existing plans for establishing databases with information on beneficial owners in the context of the transposition of the fourth Directive.

For example, a respondent to the Survey has indicated that, while "the FIU has direct access to the (…) Companies Registration Office", it is "only a register for registered members of the board and companies annual report"; in the next future, "there will be a register with information on the legal and beneficial ownership of companies". Another respondent equally points out that currently "data on companies are public" but "the concept of beneficial owners is unknown in our law"; the new upcoming legislation will require the collection of "data on beneficial ownership which will be accessible for law enforcement and obliged entities".

While the vast majority of EU FIUs can have access to national registers of companies, the content of such registers and the information that FIUs can extract from them differ to some extent across Countries. According to responses, information on directors is commonly accessible; other available information includes accounting and corporate documentation.

Examples taken from responses refer to the following types of data obtainable from the companies register: "Incorporation acts, extracts of documents from foreign commercial registers when a foreign entity participates in the management or ownership of a [national] company, financial statements, shareholders lists, protocols of General Assembly of the company, information on accumulative bank accounts for the registration of a company and other financial and administrative documents".

Or, in another case: "Trade name and registered company name trade name and registered

[96] Possible mechanisms envisaged by the FATF (Recommendations 24 and 25 and their Interpretive Notes) include obtaining beneficial ownership information from entities obliged to acquire them through CDD, using law enforcement powers, setting up central registers or a combination of those.

company name; registered address; legal form; date of registration (…) and date of incorporation; duration; corporate capital and to what extent it has already been called up; financial year and annual accounts (consolidated accounts if applicable); corporate object; director(s) name(s) and address(es); shareholder(s) name(s) and address(es); delegation for daily management if applicable; external auditor(s); branch(es); merger(s); articles of incorporation and its various amendments; ordinary and extraordinary shareholder meeting(s) and resolution(s); director(s) resolution(s)".

In some cases, respondents also inform about their access, besides information on companies, to data concerning other legal entities (e.g. associations, foundations, not-for-profit organisations).

A respondent to the Survey refers to the FIU's access to, i.a., "databases on financial reports of companies and NPOs, NPO registry maintained by the Ministry of Finance, Associations Registry and Foundations and Endowments Registry" maintained by another competent ministry.

Importantly, although only a few, some FIUs cannot obtain information on the legal ownership of companies. They are therefore prevented, based solely on the consultation of companies register, from identifying shareholdings and determine the property structure of legal entities.

No reference has been found, in responses, to access specifically to information on trusts or similar legal arrangements[97].

As regards the access procedures to companies' information, this is most of the time based on electronic direct means of consultation, which allow the FIU to obtain the requested data immediately[98]. In some cases, though, especially in countries where the central register does not hold all needed information and different sources have to be used (e.g. notarial databases have to be consulted or obliged entities have to be approached), access procedures may vary and the related timeframes may be longer.

In these cases, in fact, respondents indicate for example that "information on the legal ownership of companies may be obtained instantaneously as it is available online. Information on beneficial ownership may take a few days". Other responses point out that beneficial ownership information "has to be requested by a written formal request", which is "usually answered within a month".

7.1 Other information sources on legal and beneficial ownership

Despite the absence to date of proper central databases with complete information on beneficial ownership, some FIUs highlight that they can anyway obtain this information, as needed for their analysis and international cooperation, through other registers with relevant data or by using other means.

A particularly important role seems to be played in these cases by notaries as, in countries that have a notarial system for the setting up of companies and other legal entities and for changes related to their ownership or corporate structure, these professionals are not only required to acquire

[97] On this point, on the contrary, a respondent has explicitly highlighted that "trusts are not recognised in the [national] legal system and no such register is established.

[98] A respondent informs that its access to the information on the legal ownership of companies is "semi-direct from a third party (Tax Authority) via a Web application"; the information is received "the following day after the request has been sent".

beneficial ownership information (notably to perform their CDD duties) but are also obliged to provide this information upon request by the FIU and other competent authorities.

A respondent to the Survey informs that "the self-regulatory body of notaries holds a database with information on beneficial owners", which can be accessed by the FIU. The same respondent, while flagging that "we still need to implement the register envisaged" in the Directive, also notes that "in the Accounts' Holders Database we have recently set up, one of the compulsory fields is for the identity of the beneficial owners" (it is not clear, though, if this information is about the beneficial owners of the accounts or of the companies holding the accounts).

Another respondent (which also underscores that "a central beneficial owner register is going to be set up for the transposition of the fourth Directive") also highlights that the FIU "has access to the data held in the register on companies, as well as to the information recorded by Notaries. The FIU has also access to information on beneficial owners of companies, trusts and other legal arrangements held by relevant reporting entities, which can be identified also through the account and deposit databases".

A mixed approach to obtaining corporate information, including on beneficial ownership, is also followed by another FIU that points out that "information on the legal ownership of legal entities is publicly available online at the [companies register]. Information on beneficial ownership must be collected from all agents (…) of the concerned company/trust/other legal arrangement", as the FIU "may contact any reporting entity with a request for information".

7.2 Conclusions on access to information on legal and beneficial ownership

Responses show that the obligation for Member States to set up central registers with beneficial ownership information, as provided for by the Directive, is yet to be fulfilled. Concerns may arise on the capacity to properly comply with this requirement within the deadline set for implementation (26 June 2017) in light of the complexities of such endeavour.

These concerns are somewhat heightened by findings that show that some FIUs may not have access to company registers in their countries and some of those that do have this access cannot obtain information on the legal ownership of companies.

As seen from the previous analysis, several FIUs rely on composite mechanisms that allow them to have access to information on companies, other legal entities or trusts based on different sources and through different procedures. These normally entail consulting separate databases or approaching certain categories of obliged entities (such as companies, trust and company service providers or financial institutions).

In this regard, it is important to underscore that only a centralised database can allow FIUs to determine if an individual holds beneficial ownership positions, what are the interested entities or legal arrangements and what are the characteristics of the beneficial ownership itself. Other, "decentralised" means, such as the capacity to obtain information from obliged entities (banks, notaries), presupposes that the FIU already knows where the relevant individual or entity holds a business relationships.

Another problem, as also flagged by respondents, is that information gathered by obliged entities may not be complete or duly updated.

8. Other financial and administrative information

Essentially all EU FIUs have indicated that, in addition to data on bank accounts, other assets and beneficial ownership (with the constraints and limitations discussed in previous paragraphs), they can access other, additional types of financial and administrative information to pursue domestic analysis and FIU-to-FIU cooperation. These additional sources of financial or administrative information are particularly numerous and diversified across EU FIUs, although several commonality are easily identifiable. The following points summarize and describe the information sources that, based on responses, are most commonly available to FIUs or are specifically useful in support of their activities.

- **Population registers/databases or general registers of natural and legal persons.** Information on the identity of nationals or residents, relevant identity documents released and their terms of validity, parental relations. Some respondents also indicate that they have access to registers with information on holders of driving licences.

- **Social security databases.** Information on resident population, on legal persons' number of employees, wages, social security allowances.

- **Tax and revenue databases.** Tax information on natural and legal persons, concerning declared incomes or assets, amounts due or paid and related complaints or proceedings. Responses also refer to information on VAT, outstanding tax debts, number of employees and their salaries.

- **Immigration, aliens or asylum seekers registers.** Information on residence permits, immigrants, individuals applying for asylum.

- **Passports and visas database.** Information on passports and visas issued by competent national authorities and their holders.

- **Travel information.** Data on individuals travelling to or from third countries.

  In addition, an FIU has informed that it has access to a "car registration plates' database" concerning "all cars crossing the borders". As also highlighted in several responses, vehicle registers are frequently available to EU FIUs.

- **Credit exposures.** Information on natural or legal persons' financial obligations (e.g. outstanding loans, mortgages) and possible defaults.

  Responses to the Survey on this point show that some FIUs have access to central credit registers on present and past credit exposures to financial institutions and the related defaults.

- **Wire transfers.** Information on transfers of funds performed through banks.

  A respondent has indicated that it has access to TARGET2 (Trans-European Automated Real-Time Gross Settlement Express Transfer System), a database which stores all data pertaining to wire transfers in the euro area.

- **Weapons registers.** Information on persons authorised to carry firearms or on prohibited weapons.

Other, perhaps less common, sources of financial or administrative data available to some FIUs are related to information held by utility providers[99], information on employment histories of individual workers, information on companies listed on the stock exchange and on licensed and regulated financial institutions, information on local politicians or public administrators.

Also due to the considerable diversity of these sources of information, access procedures for FIUs vary accordingly. In cases where the information is gathered in central databases (such as population or tax registers), the FIU can normally gain direct access through electronic channels; responses are therefore received immediately upon request. However, in some cases the information can be obtained only indirectly by the FIU, based on appropriate requests filed to the competent institutions that hold it.

FIUs explicitly highlight in their responses to the Survey on this point that "access is received on foot of formal requests", even though "there is no restriction on information that can be provided". In other cases, "access to such information, depending on the sources, is either direct to the relevant database or indirect through competent authorities". Similarly, another response points out that "access is direct to the relevant database or indirect through competent authorities when the needed information is classified".

Clearly, when the access by the FIU is only possible indirectly following ad-hoc requests, this may entail longer timeframes for the FIU to obtain the information. On the other hand, based on responses, forms of indirect access do not seem subject to particular forms of discretional evaluation by the authority that holds the information.

On the timeframe for obtaining the information in response to requests (in cases of indirect access), respondents indicate, for example, that although "there are no set timeframes", "two week is probably the norm". Others mention "few days" for receiving information in such cases.

8.1 Conclusions on access to other financial and administrative information

The survey shows that the range of financial and administrative sources of information available to EU FIUs is particularly diverse, also reflecting the FIUs' different natures and objectives underlying the common functions of "analysis". While this range appears to be generally broad, the conditions for the access are also variable and in many cases forms of indirect access seem to pose conditions to the FIUs' capacity to obtain information. Responses to the Survey do not refer to existing plans, being considered at the national level, to expand or improve the range of databases or information available to FIUs. Reference is only made, again, to the prospective setting up of central registers of bank accounts and of beneficial owners which, as discussed in the previous paragraphs, are specifically mandated by the Directive.

It is also true that, with the exception of these two types of databases, the EU provisions do not foresee particular information sources that Member States have to make available to FIUs for their analyses and international cooperation. As seen, in fact, the Directive generically requires that FIUs should have access to "financial", "administrative" and "law enforcement" information, with no description of what specific types of data should fall into these ample and not too well defined categories. The resulting discretion, together with the mentioned differences in FIUs' natures,

[99] Accessible, as reported by a respondent, "upon a formal data protection request".

organizations and analytical functions[100], appears to be the root cause for the considerable variety and diversity of information sources available to EU FIUs across Member States.

In this diversity lie problems and opportunities. As to the former, unequal capacities to have access to information may lead, domestically, to less effective analysis, in cases where the scope of available sources is reduced[101]. As regards FIU-to-FIU cooperation, FIUs with a narrow range of available databases may be less effective in providing useful information. Cooperation can also be negatively affected by the considerable differences in information accessible, for two concurrent reasons: the requesting FIU may not receive the information needed (for example, on whether a particular subject owns assets abroad) because the requested FIU does not dispose of the relevant database; or, the exchange may be refused due to the lack of reciprocity in cases where the requesting FIU does not dispose of the information sought from the requested counterparts.

As indicated, differences in available databases also offer opportunities deriving from the identification of good practices which can be shared among Member States and FIUs, thus assisting in identifying information needs in support of quality analysis and cooperation and ways to satisfy those needs.

More detailed provisions or indications at the EU level on types of information which qualify as "financial" or "administrative", in addition to that related to bank accounts and beneficial owners, would certainly facilitate this process of better alignment and improvement of the range of domestic databases available to FIUs. For this purpose, further work needs to be done on the identification of types of financial and administrative information that EU FIUs have access to.

This work may provide useful indications on existing practices and may also allow to identify examples that can be used to set a common framework of reference for Member States and FIUs to shape the set and scope of information sources that, in addition to registers of bank account and beneficial owners, should be available to FIUs for their analysis and cooperation. Such a common framework of reference, besides possibly assisting EU Countries and FIUs in national implementation of international and EU provisions, may help reducing differences and discrepancies among EU FIUs that affect both domestic functions and FIU-to-FIU cooperation, this latter also via the possible application of the reciprocity condition.

It is also important to improve conditions and procedures for FIUs to have access to available databases. Based on the findings from the survey, access can be sped up, particularly through the use of direct electronic connections, and made less dependent on decisions by the authorities that hold the relevant information.

9. Law enforcement information

The issues outlined above in relation to the availability of, and access to, types of financial and administrative databases are also true to a considerable extent when it comes to law enforcement information. Faced with an equally general and undefined notion in the Directive, Member States

[100] See Chapters 1, 2 and 5.

[101] It has to be recalled that the range of the information to which the FIU can have access is not the only factor influencing the FIU's capacity to develop analysis. In fact, as mentioned above in paragraph 1, the FIU's capacity to to dispose of adequate information should be assessed in light of the number of initial disclosures (STRs/SARs, CTRs), their type and content, the extent of the power to obtain information from obliged entities, the access to external databases. This latter element, although very important, is therefore one among several factors and cannot be considered in isolation to draw conclusions on the FIU's capacity to obtain sufficient information to perform effective analysis and international cooperation.

have identified considerably different sets of "law enforcement" information available to their FIUs. Due particularly to the need, in many cases, to access sensitive information held by agencies in charge of criminal investigations or prosecutions, these differences are in several cases rooted into the difficulty for non-police-type FIUs to have access to law enforcement information or databases. This access, although only in few cases and under particular circumstances, turns out to be entirely absent.

Moreover, although the majority of FIUs have access to this category of information, both the types of data which can be obtained and the conditions and procedures for acquiring them are considerably different across Member States, with significant impacts on domestic activities and on FIU-to-FIU cooperation.

9.1 Types of law enforcement information

The range and types of police information available vary greatly, particularly as a function of the nature of the FIU and of the relations it has with law enforcement agencies that hold this information. Clearly, police-type FIUs have the broadest access, often encompassing all police databases available domestically, under the same capacity accorded to national police bodies. Hybrid FIUs rely normally on requests filed to competent law enforcement agencies or on information channeled by "liaison officers" (see the following paragraphs for more details on the different approaches to access procedures). The following points provide an overview of types of police information that are most commonly available to EU FIUs.

- **All law enforcement databases domestically available**. This particularly broad access is granted, based on responses, to several police FIUs.

> Responses to the Survey from police or judicial FIUs, in fact, state the access is extended in many cases to "all available law enforcement information". Some respondents add informative details on the specific content of main police sources available: "The FIU has direct unlimited access to law enforcement databases such as criminal records, departure/arrival records, stoplist records, the Crime Analysis Database of the Police, stolen vehicle registry and administrative information like civil registry (operated by the Ministry of Interior), investigation records"[102]. Similarly, another respondent flags that, "using automated functions", it has access to "information in the Police Authority's database as well as the criminal records register (criminal convictions), suspicions register (actively suspected crimes), the general surveillance register (intelligence information) and the central investigation register (operative register for modus operandi)". Along the same lines, another police FIU informs that it has access to the Police National Computer with information on "details of convictions; impending prosecutions; vehicle registration addresses; aliases; firearms certificates; associates; SIS alerts[103]; wanted/missing; warning markers; driver disqualification reports; subjects of interest to [national] law enforcement; outstanding court orders for restraint or confiscation".

- **Criminal judicial decisions**. These types of databases contain information on decisions taken by criminal judges or courts, including on convictions or acquittals, seizures, confiscations. In most cases, FIUs that have access to this information can obtain data on both ongoing legal proceedings and past criminal records.

[102] While, of course, clear boundaries or differentiation between "law enforcement" and "administrative" information cannot easily be established, these latter types of data recalled in the box could well be categorized as "admninistrative".

[103] Alerts from the Schengen Information System (SIS) concern categories of wanted or missing persons and objects.

For example, a respondent highlights that it has access to a "Punishment Register" with "criminal and misdemeanor punishments entered into force in [the Country] (persons punished, legal grounds, dates of punishments entering into force, sentenced punishment)". Another respondent indicates it can access information on a "person's involvement in criminal proceedings (current and historical data), convictions, etc.". Responses also make reference, in some cases, to FIUs' access to "international cases", that is information about "requests for mutual legal assistance in criminal matters", including "amount seized, confiscated, decisions [taken]".

- **Criminal investigations or prosecutions**. These databases include information on ongoing investigations or prosecutions, with details on the case, the subjects involved, the underlying criminal activities.

For example, respondents inform that they have access to "Criminal investigation databases" or "Registers" with "information on all criminal investigations conducted [in the Country] by the Police, the Customs or the Frontier Guard" or on "criminal investigation numbers and law enforcement-established legal grounds, start (and end date if not ongoing) of the investigation, legal grounds for starting the investigation".

- **Criminal intelligence**. These sources provide information on the potential criminal interest of particular subjects, also outside of formal ongoing legal proceedings or police investigations.

Responses on this point refer, for example, to "criminal intelligence" deriving from "surveillance activities". An "observation database" is mentioned as gathering information filed by police officers "possibly related to crime". Reference is also made to "Persons who are subjects of interest of the Police Force", also based on the "Schengen Information System".

Other police databases available to FIUs, although less common, are related to information on "natural persons' crossing of State Borders"[104], wanted persons, customs information.

In one case, a respondent has informed that it doesn't have access to law enforcement information for own analytical purposes, whilst this access, though indirect, is allowed when police information is requested by foreign FIUs.

In this particular case, "the law does not empower [the FIU] to have access to law enforcement information for analytical purposes", even though the same FIU receives a limited "feedback" from law enforcement agencies, on a monthly basis, "on the STRs' relevance in light of available information in police databases", based on "criminal records or ongoing investigations/prosecutions". This feedback, limited in content with respect to the information available to law enforcement agencies on the same cases, seem to follow a preliminary sharing by the FIU of the disclosures received (possibly limited to the identity data of the subjects involved) and is referred to the "relevance" of STRs as such (for prioritization purposes), not specifically to individual subjects reported as involved in suspicious activities.

The same respondent clarifies that, despite these restrictions for domestic analysis, it can access certain police information "for international cooperation purposes", that is "if explicitly requested by FIUs of other countries". The law enforcement information that can be shared under these

[104] "Domestic and foreign nationals entering/exiting [the Country] from the last 10 years, including information on the type of transport, used vehicles, passengers, points of entry/exit, used ID documents".

circumstances includes "criminal records (…), denunciations, convictions, orders of arrest or seizure measures, and the indication of the related offences".

9.2 Access procedure

As already mentioned, responses, similarly to those on the types and contents of available law enforcement databases, show that also the procedures that FIUs have to follow to access these databases vary considerably. The following overview, based on information provided by respondents, outlines the different approaches taken across Member States to allow the FIUs to have access to law enforcement information.

Modalities vary crucially depending on the nature of the FIU, its institutional setting and the relationships with police agencies: direct access is a prerogative of FIUs that have a law enforcement nature or have dedicated means of liaising and communicating with competent police bodies; indirect access can be carried out through liaison officers or by means of ad-hoc requests, filed by the FIU on a case-by-case basis. Of course, to different modalities correspond different timeframes for obtaining the information.

9.2.1 Direct access

Police FIUs, set up themselves as specialized law enforcement bodies or otherwise located into national police agencies, have generally ample and direct access to any law enforcement database. This access is normally possible through electronic means or "online" modalities. Some hybrid or administrative FIUs can also use direct electronic means of communication to obtain information from accessible police databases. It is also important to emphasize that, while in some cases all FIU staff can access available police databases (for police-type FIUs), in other cases such access is reserved to staff members with appropriate levels of clearance.

Responses to the Survey on this point refer to "dedicated communication channels", based on "online connections". One respondent mentions a "direct access to a joint law enforcement database which allows to simultaneously conduct checks on certain targeted individuals and companies". It appears, therefore, that multiple databases can be interrogated through one query.

Interestingly, another respondent (also a police FIU) has highlighted that the embedment within the national police agency allows, besides the access to databases, forms of information sharing: "Given the integrated nature of [the FIU] relative to the Police Authority and the national criminal intelligence service, there are good avenues for information and knowledge sharing between [the FIU] and the latter".

9.2.2 Indirect access

The majority of administrative FIUs have only indirect access to available law enforcement databases or information. The procedure can take different forms. In some cases, liaison officers (normally police officers who have access to police databases) ensure that law enforcement information is extracted from relevant databases and provided to the FIU on a "need-to-know" basis in support of analysis (or FIU-to-FIU cooperation).

For example, a respondent to the Survey informs that the FIU receives police information based on "indirect access through liaison officers and/or magistrates who are part of our staff[105]". In another

[105] This respondent also informs that the "next step will be to allow the FIU to have direct access to police databases".

case, the information is obtained "through the units of the National Police and Civil Guard within the FIU. A mixed approach is applied by an FIU that "has direct access to information on judicial proceedings" and "does not have direct access to the police database", which is ensured through a "liaison officer (…) whom it can contact at any given moment and is in charge of satisfying any information request from the FIU with respect to the police databases".

Other, more traditional modalities of indirect access are based on the filing of written requests by the FIU to the competent police agencies. Responses in this regard indicate that FIUs send written requests to obtain information, for example, on criminal courts' decisions.

More broadly, an FIU informs that "law enforcement information is obtained (…) by virtue of requests for information". Another FIU recall that "law enforcement information is not directly available to [the FIU] and has to be sought by approaching competent law enforcement agencies" by means of ad-hoc requests.

9.2.3 Timeframe

The type of access procedure clearly affects the timeframe within which FIUs can obtain law enforcement information. All respondents that have reported forms of direct access to police databases through electronic means have confirmed that they can receive information promptly, essentially in real time. FIUs using indirect means of access have normally to wait longer.

Liaison officers ensure a quick feedback ("quasi immediate", as referred by a respondent), while feedback to written requests is normally received after a longer delay: responses indicate a range comprised between one week and "about 30-60 days". While this latter timeframe appears particularly and excessively long, several respondents recall that information can be obtained more rapidly in cases of urgency.

9.3 Conclusions on the FIUs' access to law enforcement information

In the absence, in the Directive, of a definition of "law enforcement" information setting the scope of data which, as a minimum, should fall into this category and be available to FIUs in support of their functions, the survey has highlighted the existence of a considerable variety across Member States of available law enforcement databases. It has also shown cases of difficulty for EU FIUs to have access to a sufficiently broad range of law enforcement information.

There is a considerable "gap" between police or judicial FIUs, that can access a wide array of domestically available police databases, and administrative and hybrid FIUs, with a more limited access. Most relevant limitations seem to lie in the availability by the latter FIUs of information related to ongoing investigations or prosecutions, as well as on intelligence gathered outside of legal proceedings or formal criminal investigations.

The same considerations developed in the previous paragraphs as regards the scope and differences of "financial" and "administrative" information can be recalled here on the FIUs' capacity to have access to law enforcement information. The following points need to be more specifically reiterated.

- Existing limitations may impact on the FIUs' capacity to perform effective analysis at the domestic level and to provide a sufficiently broad cooperation to foreign counterparts.

- In this last respect, possible negative implications triggered by the reciprocity condition cannot be underestimated.

- The conditions and procedures for allowing the FIUs' access to law enforcement information also vary considerably, with forms of indirect access which may entail difficulties to obtain timely information.

- Remaining cases where FIUs do not have access to law enforcement databases or information (particularly, as seen in previous paragraphs, for domestic analysis) should be urgently addressed and solved through appropriate action by the interested Member States.

- Indications crafted at the EU level on what types of law enforcement information should be available to FIUs as a minimum would be particularly helpful to foster uniform implementation, approach national solutions and mitigate the undesired effects highlighted in previous points.

- For this purpose, further work may be considered to more precisely and completely map out police sources that are currently available to EU FIUs and to identify practices which could be shared and implemented across Member States.

CHAPTER 4

FIUs' POWER TO OBTAIN INFORMATION FROM OBLIGED ENTITIES

1. Introduction. Scope and purpose

The last sentence of article 32(3) of the fourth Directive makes it clear that Member States have on obligation to empower their FIUs "to obtain additional information form obliged entities". This power enlarges the sources of information that FIUs should be able to access to perform their tasks: the capacity to approach obliged entities and request information is additional to the availability of "financial, administrative and law enforcement information" obtained from external sources, separately referred to in article 32(4) (and dealt with in Chapter 3 of this Report).

As regards the scope of the FIUs' power to obtain information from obliged entities, article 32(3) first clarifies that this information is "additional". This provision, therefore, seems to assume that requests to obliged entities are intended to provide FIUs with further elements on cases that are already under the FIUs' scrutiny, either because an "initial" (as opposed to "additional") disclosure has already been filed or because the FIU has otherwise initiated an analysis[106]. In any event, it appears that requests should be possible and allowed when the FIU already possesses "initial" information on a case that needs to be further enriched or analysed.

It is important to underscore upfront that the source of this information does not have to be necessarily on STR or a SAR (as will be discussed in the following paragraphs, the existence of prior STRs/SARs is in some cases a pre-condition for the FIU to be able to exercise this power); any other types of information qualifies as well to trigger the power to obtain additional elements from obliged entities, either coming from domestic sources (for example, inputs provided by other authorities, threshold-based disclosures, data obtained from open sources) or from foreign agencies (typically, communications from other FIUs).

Given the particularly broad spectrum of sources originating "initial" information that is eligible to trigger the FIUs' power to obtain "additional" elements from obliged entities[107], it can be safely said that FIUs should be able to obtain information from obliged entities, in accordance with paragraph 3 of article 32 of the Directive, whenever they are performing their analytical functions as mentioned in the same paragraph (as well as, based on article 53(2), to respond to requests from

[106] This of course without prejudice to the duty for FIUs to obtain information from obliged entities upon requests from foreign counterparts, regardless of whether domestic disclosures have been received or analyses have been started, in accordance with article 53(2) of the Directive.
This point will be discussed in Chapter 6, where the existence of limitations and constraints will be highlighted. As will be illustrated in this Chapter, conditions and limitations apply also to the exercise of this power for domestic purposes.
[107] This scope can be well determined at the domestic level, either implicitly or explicitly, based on the laws regulating the FIU's functions.

foreign FIUs)[108], that is when they are examining cases to determine whether they are suspicious and deserve further examination or treatment through dissemination and ensuing investigations. It is also important to note that the power to obtain information from obliged entities should be available to FIUs throughout the entire analytical cycle, until dissemination: either at its inception, when there is a need to determine whether a case is indeed "suspicious" and qualifies for further scrutiny, or more towards the end, when it is important to complete the analysis and gather information capable of properly steering any possible further action after dissemination.

Still on the scope, the reference to "obliged entities" clarifies that FIUs should be able to obtain information from any of the subjects that, based on the Directive and on national implementing provisions, are bound by AML/CFT obligations: the only requirement is therefore that the entity the FIU approaches with the request is included in the scope of application of AML/CFT provisions, regardless of whether or not this same or any other entity has filed an STR/SAR on the case to which the request may refer.

This important element can be further illustrated, by contrast, through reference to the correspondent FATF standard. Differently from article 32(3) of the Directive, the FATF Interpretive Note to Recommendation 29, Section C(a)(5), requires that FIUs should have the capacity to obtain information from "reporting entities": this may imply that, under the FATF standards, this FIU's power can only be exercised vis-à-vis entities that have reported a case (through an STR/SAR) or, more generally, in instances where a report has already been filed to the FIU on the same case to which the request refers (even though by a different entity).

While this FATF standard has in fact been construed in some cases as only setting a narrow scope for the FIUs' power to request information, limited to entities that has already filed a report or to cases where prior disclosures had already been received by the FIU, a different interpretation was also possible whereby the reference to "reporting entities" is considered equivalent to that to "obliged entities". Referring to these entities as "reporting" can in fact only be dependent on the particular context, which is about cases where the FIU approaches relevant subjects under the particular angle of its analytical purposes related to potential money laundering or terrorist financing activities for obtaining data or "reports"; such entities are therefore not evoked as subject to the overall set of AML/CFT obligations. This broader interpretation of "reporting entities" as equivalent to "obliged entities" has then been recently sanctioned by the FATF.

Against the global FATF standards about the scope of "reporting entities" that FIUs should be able to approach, as specifically interpreted, it is certainly safe to conclude that, under article 32(3), last sentence, of the fourth Directive EU FIUs should be able to obtain information from any obliged entity, regardless of the existence of prior disclosures, either filed by the same subjects that FIUs intend to approach or by any other obliged entity. This means, in conclusion, that FIUs can exercise this power: whenever they are considering a case in their analytical function, under whatever stage of the analysis[109] and vis-à-vis any of the entities that are subject to AML/CFT obligations that appear to hold the information sought; regardless of the existence of prior STRs/SARs or other disclosures (either from the same entity approached or by any other)[110].

[108] A different, narrower interpretation was possible under the previous third AML/CFT Directive (2005/60/EC): article 21(2) stated that FIUs should be able to receive "and, to the extent permitted [by national law]", request "disclosures of information which concern potential money laundering" or terrorist financing.

[109] And, again, for FIU-to-FIU cooperation.

[110] This means, for example, that FIUs, in order to properly analyse a real estate transaction, should be able to obtain information from the bank where a transfer has been originated based on a disclosure receveived from the bank of the recipient, in order to "follow the money" and trace them back to their possible illicit origin.

2. EU FIUs' capacity to obtain information from obliged entities

Against this broad and articulated background set by the fourth Directive, responses to the Survey show that EU FIUs still face significant constraints in the exercise of their powers to obtain additional information from obliged entities. These constraints derive from lack of full capacity or, in most cases, from the existence of multiple conditionalities.

All respondents confirm that, in general, they have the capacity to "obtain information from any obliged entities" (subject to the condition that will be recalled shortly). This capacity may be limited, in some cases, by constraints deriving from general domestic laws or procedures, for example on data protection. The information power also appears in some instances not fully and unconditionally conferred upon the FIU.

For example, a respondent has clarified that, while there are officers who are accredited to speak to banks directly on financial enquiries, they "can currently request details under the Data Protection Act and Crime and Courts Act". The same respondent also indicates that "responses vary from reporter to reporter" and the [legislator] "is implementing a power for FIU to compel information, but details [are] still to be determined".

FIUs may also lack the capacity to obtain information from obliged entities or be subject to particular conditions or restrictions in cases where investigations or legal proceedings are underway involving the same or related activities or subjects. These limitations seem to apply despite the need for the FIU to carry out analytical activities and despite the requirement that these activities should be performed by the FIU in an independent manner[111].

On this point, a respondent specifies that "in pending criminal proceedings, the [FIU] may exercise this power only in agreement with the competent prosecution authority".

It is also important to note that, although the information gathered through the Survey does not allow to draw firm conclusions on this point, several FIUs do not act upon a dedicated legal basis specifically empowering them to obtain information from obliged entities. Rather, this power is deducted, also implicitly, from general provisions in the law assigning to the FIU an overall capacity to access external sources or to query third parties. The lack of explicit provisions in dedicated laws where the FIU's capacity to query obliged entities can be clearly and firmly rooted can give rise to uncertainties or undue limitations, especially when the access to information held by obliged entities has to be checked against other, potentially conflicting requirements (such as those about data protection or financial or professional secrecy).

On this point, for example, a respondent highlights that it "may collect data to supplement existing information or for the purpose of analysis by placing requests for information or making enquiries with public and non public bodies", whereas obliged entities are included among the latter.

Responses to the Survey also hints to conditions to the FIUs' capacity to obtain information consisting in the existence of a "suspicion": this has to precede the request (and possibly has to be demonstrated and substantiated to justify the request), which entails that information from obliged entities may not be obtained to establish if a particular transaction or activity of which the FIU has

[111] See Chapter 2, par. 2.5, on the requirements about the FIUs' independent functioning in relation to access to information. In this perspective, the existence of investigations or legal proceedings on the same or on related cases, while certainly requiring appropriate coordination and cooperation, should not deprive the FIU of its responsibility to pursue aby necessary analysis.

been informed is indeed suspicious. This condition seems to contrast with the requirement, noted in paragraph 1, that FIUs should be able to obtain information from obliged entities at any stage of their analysis, even when the suspicious nature of the case under scrutiny has yet to be confirmed or validated and even in order to dispel any potential relevance so that the case can be closed. The condition of the identification of a "suspicion" in order to obtain information from obliged entities can also pose undue limitations to the exercise of this power in the context of FIU-to-FIU cooperation if the requested FIU has to verify or assess, based on its own judgment, the suspicious nature or relevance of the case to which the request refers[112].

For example, an FIU has indicated that it may order reporting entities to supply all data required for money laundering and terrorist financing prevention and detection in instances when suspicion of money laundering or terrorist financing do exist and when the FIU has already received a previous report/disclosure, such as for example a cash or suspicious transaction report from a reporting entity or a written request or a suspicious transaction report or a notification on suspicion of money laundering or terrorist financing from a foreign financial intelligence unit, a written report on suspicion of money laundering and terrorist financing from government bodies, courts, legal persons with public authorities.

Similarly, other respondents inform that they can "obtain financial and other data from obligated institutions (…) whenever suspicions of ML/TF exist".

More in general, several responses confirm that the power to obtain information from obliged entities can only be exercised by the FIU in the performance of its analytical functions related to potential cases of money laundering or terrorist financing. While this general condition does not seem to translate into undue constraints for FIUs, it is no other than a manifestation of the overarching "purpose limitation" that underlies all FIUs' activities and powers: as discussed in Chapter 1, these are focused on analysis concerning potential money laundering or terrorist financing cases and are separate from, and do not extend to, law enforcement activities or matters outside money laundering or terrorist financing.

3. Triggers and conditions

As regards the scope of EU FIUs' capacity to obtain information from obliged entities, specifically in relation to relevant triggers that allow FIUs to exercise this power, significant differences are emerging from the responses to the Survey. Responses particularly show that, while some FIUs have a broad capacity to approach obliged entities in carrying out their functions, they are subject to conditionalities of different nature.

3.1 Broad capacity to obtain information from obliged entities

Some respondents (a minority of EU FIUs) flag that they can request information to obliged entities whenever this is needed in order to perform their functions. No particular condition or requirement is attached to the exercise of the power, which is neither limited in the scope of the entities that can be approached nor subject to the existence of prior disclosures or particular information needs.

These are cases where the FIU simply can "demand information from any obliged entities as long as the information is required in order to fulfil its functions", as established by the law. Another respondent, along the same lines, indicates that it "may request the obligated persons to provide all

[112] On this particular point, which is crucially relevant for FIU-to-FIU cooperation, see Chapter 6, paragraph 2, where existing constraints are identified and discussed.

information required for the performance of their duties, including grouped information about certain categories of transactions or activities of domestic or foreign natural or legal persons".

More explicitly, the power to obtain information from obliged entities can be exercised any time this is needed to perform proper analysis, regardless of the type or nature of the trigger upon which the FIU is acting. Notably, as a consequence, the FIU is not conditioned by the existence of a prior STR/SAR, by the same entity that should be approached or by any other, and is not required to provide ad-hoc motivations for the request to obtain information, other than the need for this information to support its analysis.

A respondent clarifies that "any time an analysis is started, either based on a disclosure filed through an STR or on information acquired through other means or channels, [the FIU] can make use of its entire toolkit and activate the full set of its information powers. These include also the possibility to obtain information from any obliged entity, regardless of whether or not the requested entity has filed an STR on the case which is subject to analysis and regardless of whether or not an STR has been filed altogether". This respondent also indicates that "no particular precondition (e.g. prior STRs) or limitation is established in order to obtain any information that is relevant for the analysis. Moreover, no motivation has to be provided to the requested entity: The answer of the obliged entity is mandatory, on penalty of administrative sanction".

3.2 Existing conditionalities (existence of prior STRs/SARs; need for court orders)

Several respondents inform that their capacity to obtain information from obliged entities does not cover all instances where this information may be needed to perform analysis but can only be exercised for specified particular purposes or under certain conditions. The most relevant and widespread conditionality, based on the responses to the Survey, is the existence of prior disclosures on the same case for whose analysis additional information should be sought from obliged entities. Several FIUs can only approach obliged entities with requests for information if prior STRs/SARs have been received on the same case. Importantly, there are no cases reported by respondents where FIUs can only ask information to the same entity that has filed the disclosure under analysis; therefore, although a prior STR is required, information can then be sought from any entity subject to the AML/CFT regime.

Some respondents point out that the condition of a prior report received on the same case is not only satisfied by STRs/SARs sent by reporting entities but can also be equally fulfilled when the case is brought to the attention of the FIU through other means, typically through requests or exchanges with foreign counterparts. The information power, therefore, can be exercised by the FIU under a broader scope in these cases; obliged entities can be approached whenever the FIU has already been apprised of potential money laundering or terrorist financing activities. The broader the range of relevant sources through which the case should be reported to the FIU, the broader also the scope of its capacity to obtain information from obliged entities. In some cases, where the former is particularly wide, the FIU may find itself in a position to be able to request information whenever an analysis is started, based on any information source; the conditionality of prior disclosures may become "diluted" and, like in the instances recalled in the previous paragraph, the FIU may be able to exercise this information power whenever this is needed to pursue its analysis.

On this point, a respondent has pointed out that, in accordance with national law, "when the [FIU] receives a STR or when from information in its possession it suspects that a transaction involves ML/FT or that property may have derived directly or indirectly from or constitute the proceeds of criminal activity, the [FIU] may demand to obliged entities any additional information that may deem useful".

The condition of prior STRs/SARs being received on the same case seems to play a significant role in narrowing down the scope of EU FIUs' capacity to obtain information from obliged entities. Although less frequent, other, even more stringent, conditions apply to the exercise of this power by FIUs.

In some cases, the FIU can only approach reporting entities to obtain follow-up information on prior disclosures that are unclear or incomplete. More than a power in support of the FIU's analysis, these types of requests seem rather intended to complement the general reporting obligation by conferring to the FIU a capacity to request data instrumental to fill in missing parts of previous disclosures.

"Where a report is incomplete, the FIU will directly ask the reporting entity to provide the missing information, to make it possible for the FIU to conduct a relevant analysis of the material".

Moreover, cases are reported by respondents where the FIU is not able to request information to obliged entities without having obtained a court order to that effect, that makes the request enforceable.

A respondent indicates that "when the FIU needs to obtain further details or information from third parties, including other entities obliged to report suspicious transactions who have not done any reporting in the specific case, it may be necessary, in order to protect legal certainty, to obtain a court order".

These are cases where the FIU seems to lack entirely the power to obtain information from obliged entities or, otherwise, to be subject to prior authorization or clearance for the exercise of this power through a court order that gives validity to the request and makes it enforceable. Besides limiting or conditioning the FIU's capacity to obtain information from obliged entities, the need for an order by a third party also adversely affects the FIU's status of independence in the exercise of its functions[113].

More specifically, the lack of empowerment of the FIU in these cases, and the "substitution" of its decision with an order by a court seems to underlie an assumption that obtaining information which is hold by obliged entities is a measure that falls into the domain of law enforcement and, as such, requires duly consideration and decision by competent judicial authorities. These may be called on to assess if the case is sufficiently substantiated and justifies a derogation to general confidentiality safeguards or perhaps financial or professional secrecy regimes.

On the contrary, the provision in article 32(3) of the Directive requires Member States to assign this information power to their FIUs as an administrative tool (which should not raise any law enforcement implication) specifically in support of their analyses (that is, prior to and outside of any possible investigation or legal proceeding).

Finally, as regards the procedure for obtaining information from obliged entities, responses to the Survey confirm that this is based in almost all cases on direct transmissions between the FIU and the requested entities. Similarly to the reporting procedure for certain categories of professionals, where self-regulatory bodies of the professions concerned may be interposed between the reporting entities and the FIU, in some cases the additional information can also be obtained by the FIU through these self-regulatory bodies.

[113] See the discussion on this point in Chapter 2, par. 2.5.2.

For example, a respondent has indicated that it "can obtain information from lawyers and public notaries via the self-regulating bodies (chambers) of these professions".

The communication channels and the modalities used to approach the obliged entities and transmit the information requested generally reflect those applied for the disclosure of STRs/SARs.

A respondent has pointed out that it directly "contacts the money laundering reporting office of the obliged entities of interest" for the requests to obtain information; "thanks to this informal procedure, the analyst can make requests in a swift way and get information rapidly and directly".

4. Conclusions

Responses to the Survey show that EU FIUs generally still lack an adequate capacity to obtain information from obliged entities. Moreover, when they dispose of this power, its exercise may be subject to significant conditionalities that reduce its scope. It is of course important to take into account that the provisions of the fourth Directive have brought significant innovations on this point, as article 32(3), last sentence, sets this FIUs' power under broader terms than the previous corresponding provision in the third Directive[114]; while transposition into national laws may still be ongoing, the following points should nonetheless be highlighted for further consideration.

Insufficient capacity of EU FIUs to obtain information from obliged entities. Not all EU FIUs seem yet to be empowered to approach obliged entities with requests for information. This shortcoming may certainly have an impact on the capacity to carry out effective analysis and provide cooperation to foreign counterparts. It needs to be addressed urgently, bearing in mind that the power to query obliged entities was not only foreseen already by the previous third Directive (although in a less incisive form) but has also become a mandatory requirement under the global FATF standards since 2012[115]. Against this background, the appropriate empowerment of the FIU is certainly an issue of national implementation. However, clearer EU provisions would be helpful to clarify that this FIUs' power should be reflected in national laws in a sufficiently harmonised manner (also to avoid discrepancies that might adversely impact, besides the effectiveness of domestic analysis, good FIU-to-FIU cooperation within the EU), that it is not conditional to prior STRs/SARs or subject to other undue limitations (see the following points), thus allowing a common understanding on its scope and a similarly common approach to domestic transposition.

Lack of a dedicated legal basis. As seen in previous analysis, in some cases the FIUs' capacity to obtain information from obliged entities is not reflected in national laws explicitly providing for and regulating this power. FIUs may sometimes rely on general national provisions allowing them to query external sources or third parties. The lack of a dedicated legal basis empowering FIUs to obtain information from obliged entities can raise doubts on the existence and extent of the FIUs' capacity to receive information needed for the analysis and for FIU-to-FIU cooperation, as well as potential conflicts with other general domestic laws, restrictions or requirements (such as those on data protection or on financial or professional secrecy). A better national implementation by Member States should be ensured to address this issue and more firmly root this essential FIUs' power into a well-identified and dedicated legal basis.

[114] It is also important to recall that the Proposal for a new directive amending the fourth AML/CFT Directive brings these innovations perhaps further, particularly by clarifying that FIUs should be able to obtain information from "any" obliged entities, that is beyond those that may have reported STRs/SARs.
[115] See the Interpretive Note to Recommendation 29, as already recalled.

Existing conditionalities (prior STRs/SARs; prior suspicions). Conditions limiting the EU FIUs' capacity to obtain information from obliged entities should be removed. Similar to the access to other sources of information (domestic or foreign), FIUs should be allowed to seek information from obliged entities whenever this is needed to perform proper analysis, and of course for FIU-to-FIU cooperation purposes. In other words, this power should be available for FIUs to exercise generally in the course of their functions, without undue limitations consisting, for example, in the existence of prior disclosures on the same cases or subjects. Also, it should be clear that this power can be exercised at any stage of the FIU's analysis, that is either at its initial phase (when a full-fledged suspicion may have not yet been formed) or at its conclusion, in order to provide appropriate inputs through dissemination. No limitations should be foreseen in relation to the lack of fully substantiated suspicion, since information from obliged entities may well be sought precisely in order to substantiate (or dispel) a suspicion. While also in this case domestic implementation is crucial in properly setting these requirements in a way that ensures an ample scope for the FIU's power, common EU rules on this matter would be particularly beneficial to provide for a common framework clarifying that FIUs should be able to obtain information from obliged entities whatever this is necessary to support their functions.

Need for a court order to authorize or enforce FIUs' requests. FIUs should be able to exercise this power through autonomous and direct means, particularly without a need for a court order or other authorizing mechanisms. In fact, this power is part of the FIUs' administrative toolkit aimed at supporting its analytical functions, distinct from law enforcement activities and measures.

Distinction from law enforcement measures. It is also important to clarify that the FIUs' power to obtain information from obliged entities is specifically linked to the exercise of analytical functions and, while for this purpose it should have a broad scope, it cannot be considered a law enforcement tool and made subject to conditions and limitations consisting in the need to obtain authorizations from competent prosecutors or in constraints deriving from ongoing investigations or legal proceedings (see also the conclusions on this point in Chapter 2, in the perspective of the FIU's independence in the exercise of its information powers).

CHAPTER 5

DOMESTIC FUNCTIONS

1. Introduction. The analysis function of the FIU

Analysis, along with recipient function and dissemination, is considered as one of the three core activities of FIUs. Nevertheless, it has not been thoroughly defined in the FATF recommendations, Egmont standards[116] or in the provisions of the fourth Directive.

In line with FATF Recommendation 29 Article 32 (3) of the fourth Directive explicitly states that the FIU is the central national unit responsible for receiving and analyzing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing. The FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing.

The lack of specific provisions on what kind of activities fall within the analysis function entails a great differentiation of its concrete development by the FIUs, which is actually influenced by the nature, location and role of the FIU within its national AML/CFT framework.

Although the analysis function of the FIU is not explicitly defined in the FATF Recommendations, some further elements on the type of financial analysis that can be conducted are provided by the Interpretive Note to Recommendation 29, which distinguishes between operational and strategic analysis. Accordingly, Article 32 (8) of the Directive has introduced this differentiation, defining the two types of analysis as follows:

- **Operational analysis**, which focuses on individual cases and specific targets or on appropriate selected information, depending on the type and volume of the disclosures received and the expected use of the information after dissemination.
- **Strategic analysis,** addressing money laundering and terrorist financing trends and patterns.

Also the requirement pursuant to the FATF standards and the Directive – article 32 (3) - on the operational independence and autonomy of the FIU entails the capacity of the FIU to take autonomous decisions to analyse, request and disseminate specific information. This guiding principle implies the possibility of adopting a selective approach towards the information taken into account for analysis and further dissemination. In this respect, the interpretive note to FATF recommendation 29 highlights that an FIU analysis should add value to the information received and held by the FIU. While all the information should be considered, the analysis may focus either

[116] In this respect, references to the analysis function of the FIU can also be found in other publications, such as *Operational Guidance for FIU Activities and the Exchange of Information* issued by the Egmont Group.

on each single disclosure received or on appropriate selected information, depending on the type and volume of the disclosures received and on the expected use after dissemination (…). The need for implementing a selective approach in the analysis is also a pressing operational need, as underlined in Chapter 2, to cope with the constant increase of the suspicious transaction reports received and other relevant information concerning money laundering, associated predicate offences and terrorist financing. In this context, the suspension of a transaction represents a very important administrative tool of the FIUs, which allows to respond adequately to cases of particularly high risk.

It is therefore of utmost importance in order to effectively prevent criminal activities that STRs are timely sent to the FIU, even before the execution of the transaction and that the FIUs are empowered to take urgent action to promptly react, also on behalf of foreign counterparts, where for example the suspicious transaction requested, interrupts the paper trails of funds that are likely to be of criminal origin, hampering their possible seizure.

Taking into account that the AML/CFT reporting system is more efficient if the disclosures are made in a timely manner, the suspension of a transaction represents a very important administrative tool for the FIUs. This important tool allows the FIUs or, where appropriate, other competent authorities, to have an immediate reaction and to respond adequately. This report intends to emphasize the fact that the principle of reporting before the execution of the financial operation should be used as a general rule and not as an exception.

Taking into account the vital role of both analysis and dissemination in FIU activities, the report focuses on these functions, particularly in relation to the following aspects:

- FIU capacity to perform operational analysis and select relevant cases for analysis;
- the capacity of FIUs to conduct strategic analysis;
- the type of disseminated information;
- FIU capacity to provide information in response to requests from competent authorities.
- the capacity of the FIU to postpone suspicious transactions

2. Operational Analysis

2.1 Capabilities regarding operational analysis

Based on the answers provided in the survey, all FIUs declared that they conduct operational analysis, focusing on individual cases and specific targets. The analysis of particular targets (people, assets, criminal networks and associations) aimed at determining the links between those subjects and possible proceeds of money laundering, predicate offences or terrorist financing is also the main reason for interaction with foreign counterparts or other domestic law enforcement authorities.

While operational analysis is a common feature for all EU FIUs, its character and objectives vary considerably in different Member States.

The structure, tasks and status of the FIU has a significant impact on the sources of information available for analysis, its purpose and the possibility to exchange this information with foreign counterparts. A review of the responses to the survey identifies two key aspects that must be highlighted in this context.

a) Sources of information available to FIUs. The range and timeliness of information available greatly influence the character of the analysis conducted by FIUs. In this respect, there is a significant difference in the variety of information available to FIUs. While all FIUs receive disclosures on suspicious transactions from reporting entities, there is no common approach to the format and information included in such disclosures, which results in different models and templates used throughout the EU. Furthermore, the range of information that should be available to FIUs to fulfil their tasks properly, i.e. "the financial, administrative and law enforcement information" is only vaguely provided under the Directive (art. 32 (4)). Similar differences can be identified as regards the form (direct, indirect) and timeframes of access to such data by the FIUs, as highlighted in Chapter 3.

b) The need for a clear distinction between analysis and other activities – in particular investigation and other law enforcement activities. FATF recommendation 29 highlights the need for each Member State to have a financial intelligence unit with defined core functions, distinguishing the aforementioned activities of the FIU from tasks assigned to law enforcement and prosecution authorities. This indicates that the FIU analysis should be clearly a separate function from investigation. As detailed under Chapter 1 however, in financial intelligence units with a law enforcement or judicial status, these activities may overlap. The lack of a clear distinction between these two tasks may have a negative effect on the power of these FIUs to obtain necessary information from reporting entities and be able to cooperate with counterparts, especially in situations where a criminal investigation has been initiated. The aforementioned overlapping between analysis and investigations functions may also orientate financial intelligence unit analysis mainly towards suspicious activity linked to ongoing criminal proceedings.

2.2. Separation between analysis and law enforcement activities

As said, FIUs' analytical functions are distinct from law enforcement and prosecutorial activities conducted on the same phenomena. The former are, in fact, specialised, separated out and assigned to FIUs as competent authorities, in turn different from investigative agencies (even when they have a police status: see Chapter 1). On the other hand, as the FIU's analysis focuses on suspected criminal cases and is performed with the aim to support ensuing investigations and prosecutions on such cases, there are of course several important connections between these activities. The relations between them are regulated mainly through the dissemination of information by the FIU: either spontaneously or upon request[117], the FIU forwards STR information and the outcomes of its analysis to competent law enforcement bodies precisely to allow them to initiate proper investigations (or support existing ones).

These relations between analysis and investigation may become somewhat more difficult to discern, or blurred, in cases where the FIU has itself a police status, or is located in a police or judicial organisation. The closed proximity between the analysis and the investigative stage, or their assignment to the same agency, may make it difficult to draw a precise distinction between these different functions, as the two may be unified in a seamless "continuum"[118]. The dissemination itself may become difficult to identify and single out as an autonomous function, as the STR and analysis information may be simply shared or accessed (rather than proactively forwarded by the FIU) within the same organisation; or the FIU itself (or other units in the same body) may be in charge of both the initial analysis and the law enforcement follow up, thus using the disclosures and related information for both purposes at the same time.

[117] Under article 32(3)(4(5) of the Directive.
[118] This point has been discussed in Chapter 1.

The issue of the distinction between FIUs' functions and law enforcement activities is important both at the domestic level, in relation to the separation and coordination between analysis and investigation (and the availability of autonomous powers for the former), and in the area of international cooperation. On this latter aspect (which will be dealt with specifically in Chapter 6), FIU-to-FIU cooperation in support of analytical tasks must be kept distinguished from the police and judicial channels of cooperation, as the two pursue different purposes and are subject to different rules and conditions. As we will see, there are several instances where, instead, concerns related to the investigation or prosecution of crimes may be unduly anticipated at the FIU-to-FIU cooperation stage which, as a consequence, may become subject to conditions or limitations associated with the identification and nature of the underlying criminality or with the existence of criminal investigations or legal proceedings on the same facts.

Responses to the Survey indicate that for the majority of law enforcement FIUs the analysis tasks are kept separate, legally and procedurally, from investigative or judicial activities, carried out by the FIU or by the host organisation on the same facts. In two cases, however, respondents have highlighted that a clear demarcation does not exist and that, therefore, analytical and law enforcement activities overlap and are conducted in conjunction.

This point is well illustrated by a recent Mutual Evaluation Report adopted by the FATF on a Country which is an EU Member State and whose FIU has a police status. The findings of the assessment for the Immediate Outcome 6[119] highlight that the FIU "functions well as a predicate offence and associated ML *investigation* unit, rather than as a financial *intelligence* unit. The approach of the FIU with regard to STR analysis is primarily investigative (as opposed to intelligence approach) as it seeks to identify predicate offenses that could trigger a criminal case. Financial intelligence and other relevant information are rarely used in investigations to develop ML evidence".

In light of these findings, it is consistently recommended in the Report that the assessed Country "should reconsider [the FIU's] role as an investigative unit and thus make it possible for it to disseminate information to domestic authorities and foreign counterparts without first opening an investigation".

The absence of a clear distinction between analysis and investigation may affect the FIUs' capacity to perform analysis as an autonomous function. A lack of adequate recognition of the specialised nature and role of the FIU and of its tasks may deprive investigations and prosecutions of the added value that, in the logic of the Directive and of international standards, the prior analysis is supposed to bring for the ascertainment of economic and financial crimes.

Moreover, bringing forward analysis and investigation as conjoint activities may impact on the FIUs' capacity to exercise autonomous powers to obtain information from external sources (including from obliged entities) outside of a criminal investigation context and without the conditions and limitations applicable in such contexts.

As said, the FIUs' capacity to exchange information with foreign counterparts may also be affected in these circumstances (this point will be discussed in further details, in light of responses, in Chapter 6).

[119] The reference is to the FATF *Meth*odology *for assessing technical compliance with the FATF Recommendations and the Effectiveness of AML/CFT systems.*

2.3 The scope of operational analysis

While all the information received by the FIU should be considered, the analysis may focus either on each single disclosure received or on appropriate selected information. This choice should be influenced by two factors: the type and volume of the disclosures received and the expected use of the information after dissemination.

The responses to the Survey indicate that the majority of EU FIUs analyze each individual STR, whereas a significant minority only conducts operational analysis in selected relevant cases. Several FIUs have however implemented pre-analysis procedures, allowing FIUs to select cases worth pursuing. In some instances the adopted approach is differentiated according to the type of STRs received (see example below).

A respondent underscores that the type of the preliminary analysis it performs depends on the type of the reports. Some of them receive an individual treatment (they all are evaluated one by one), e.g. reports from banks. Most of the reports (reported by 'volume reporters') are processed through a 'mass process' which picks reports from the mass potentially worth opening a case. The reports are automatically compared against other databases and information (FIU databases, criminal investigation or criminal intelligence databases, etc.). The analysts then checks the possibly relevant hits (e.g. open criminal investigations, open FIU cases) and a new case is opened or the report is added to an already open FIU case.

2.4 Operational analysis – tools and procedures

The interpretive note to FATF recommendation 29 underlines that "an FIU analysis should add value to the information received and held by the FIU". In this respect, the *Operational Guidance for FIU activities and the exchange of information* published by the Egmont Group provides additional remarks as to how operational analysis can be conducted and what tools should be used:

FIUs are highly encouraged to use effective IT tools to achieve the maximum advantage in analysis. Some components of operational analysis include:

- *matching with predefined lists;*
- *identifying all reports that pertain to the same entity, on the basis of various user defined attributes, such as first name, second name, date of birth, public identification (passport number etc.), and address components;*
- *capturing all possible relationships, across multiple entities by comparing attributes such as surnames, phone numbers, addresses;*
- *analyzing relationships to form clusters of closely linked entities for various degrees of separation.*

To some extent these elements of the operational analysis are carried out by all EU FIUs. Nevertheless, the steps in the process itself and the resources dedicated to analysis- in particular IT tools – may differ significantly. In some instances the key role played by dedicated and updated IT tools to properly analyse increasing flows of information received has been underlined by respondents. The following box outline an example, provided by a respondent, of operational analysis processes based on integrated IT tools supporting the prioritization and the ensuing analysis of STRs.

The financial analysis process is divided into a series of activities designed to identify those STRs deemed to be well founded and warranting further investigation, to assess the actual degree of risk involved and to decide how they should be handled. The analysis process uses the [case management] system to gather and manage reports. [The system] also provides support for classifying reports, identifying those deemed to be of highest risk and therefore to be given priority and making the information needed for financial analysis immediately available.

Once the report is received via the electronic portal, a first phase of automatic data enrichment begins, through crosschecking structured data in the report against the information in the FIU's databases. The information then is used by [the case management system] to assign a risk rating produced by an algorithm that uses mainly quantitative variables (e.g. number of reports received on the same subject, pending legal proceedings, value of the suspicious transactions, the level of risk indicated by the reporting institution).

The system's automatic rating of 1 to 5 to each report reinforces the selective nature of the FIU's analysis. The rating is used alongside reporting entity's own risk assessment, which also employs a 5-point scale, and can be adjusted in the course of the analysis.

The STRs elaboration process is articulated in different phases:

- a first level analysis to which all reports are subjected;
- a second level analysis, aimed at an in depth study focused on more relevant contexts;
- a technical report containing the results of the analysis which is disseminated to the investigation bodies along with the related STRs.

The report is subjected to a first level analysis for a verification of the consistency between the reported circumstance and the rating. In this stage the analyst assesses the completeness of the information and understand the main information content, also taking into account any related reports. For this purpose, the analysts use their own skills and every element that is not considered by the automatic rating. Moreover, an indicator of investigative and judicial prejudice has recently been implemented, provided by LEAs on individual reports simultaneous to the first level analysis, the use of which allows to partly compensate the FIU's lack of access to the investigative databases.

At the end of this stage the analyst formulates a proposal of treatment of the report that can follow one of the following paths:

- case dismissal of reports manifestly unfounded or which do not reveal elements that can substantiate reasonable hypothesis of ML or FT;
- a simplified treatment for the reports with an exhaustive content or referred to known and recurring phenomena, as well as reports that do not require a more in depth focused analysis;
- the attribution to an analyst for a second level financial analysis, usually aimed at all the reports that require further and more in depth focused analysis.

2.5 The capacity of FIUs to focus on relevant cases

The FATF standards (Interpretive Note to Recommendation 29) establishes explicitly an interconnection between the features of the FIU's operational analysis and the type and volume of STRs received and the expected use of the disseminated information. Particular relevance is

attached to the task of the FIU to assess in which situations it should focus its analysis on each disclosure received or on selected appropriate information. As already highlighted, EU FIUs are significantly different among each other as regards their size, status, powers and processes. They also differ considerably in the types, structure and volumes of disclosures received (see Chapter 3).

The high (and increasing) number of received STRs/SARs has been identified as a challenge by several EU FIUs. To be able to carry out their functions properly, over half of the respondents have implemented a pre-analysis phase, aimed at prioritising the cases or selecting those that require in depth operational analysis. One FIU described this stage as tactical analysis – *a filter for selecting those STRs that qualify for operational analysis.* FIUs also provided examples, on the criteria that are followed to select relevant cases; the following excerpts are taken from the responses received.

> In conducting its operational analysis, the FIU examines each and every STR submitted by subject persons looking into the information received.
>
> It is only after the carrying out of such preliminary assessment based on the volume and type of information received that the FIU decides whether to go ahead or not with the proper analysis of the case or whether a spontaneous disclosure of the information received may be made to a foreign FIU.
>
> All Suspicious Activity Reports (SARs) received by FIU (around 380,000 per annum) are assessed against keyword searches and lists of known entities. Where there is a match, case by case consideration is given to next steps by officers and supervisors as appropriate. All requests for consent (giving a reporter a defense against a money laundering offence for a specific act) are given 100% scrutiny and decisions on next steps on a case by case basis by officers and supervisors as appropriate.
>
> All SARs that mention another EU member state are assessed for dissemination on a regular basis, and these are also checked against Europol databases to identify possible leads. Finally, all subjects for SARs are periodically loaded into a Ma3tch filter to enable cross-match with other EU member states.

Several FIUs indicated, that the pre-analysis procedure is mainly performed through cross checking information on subjects provided in STR/SARs with the FIUs' transaction databases, FIU case records, police and other LEA records, requests and reports from other competent authorities, information or requests from foreign FIUs and data publicly accessible.

> The Head of Department proposes to the Head of Service to open a new cases for analytical data processing based on a report of results of pre-analytical processing of data, and based on a search of the [FIU] transactions database (database of cash transactions, database of cash transfer across the border) using pre-set parameters/criteria (criterion of frequency, value of transaction, residency, records of persons already in the pending cases, etc.).

As a result of the pre-analysis procedure several FIUs assign different categories to STR/SARs in order to determine future action regarding these reports. At least two FIUs have indicated the existence of a scoring system, which determines into which category a particular STR/SAR is assigned.

> The FIU has adopted internal methodology for preliminary analysis with a matrix using criteria to establish if a STR will be further analyzed or not. According to the Preliminary Analysis Methodology, each STR receives a number of points according to risk criteria. If following the

scoring system a STR receives points above a threshold, an Operative File (OF) has to be opened. The second level of analysis (the in-depth analysis), is performed by the Department for in-depth analysis, according to Methodological Guidelines for processing of Suspicious Transactions Reports. The ultimate decision for each stage of the process (designating the report, submitting for further analysis, dissemination, etc.) is made by the Director of the FIU.

Respondents to the Survey have also indicated that the reports that through the pre-analysis stage do not substantiate reasonable suspicion of money laundering, predicate offences or terrorist financing may not be subject to operational analysis, even if they may be disseminated to foreign counterparts or competent authorities. One FIU also highlighted that STRs, which do not provide enough suspicion of ML/TF, can be rejected and returned to the obliged entity.

If there is not enough suspicion of ML/TF, the STR can be rejected and returned to the obliged entity. There is a preliminary analysis that concludes with its admission or rejection. Once it is admitted, the STR is always analysed.

The majority of FIUs are confronted with a high volume of STRs/SARs. An FIU commented that the type and volume of the disclosures received, the type of obliged entity and the expected use of the information after dissemination influence the thoroughness of the analysis conducted by the FIU – due to capacity limitations and the need to prioritize cases.

Based on information provided by respondents to the survey it seems that EU FIUs consider all disclosures received from reporting entities. Nevertheless many units are influenced to select relevant cases for operational analysis.

The type and volume of the disclosures received, the type of obliged entity and the expected use of the information after dissemination are all elements that influence the thoroughness of the analysis conducted. While all disclosures received from reporting entities are subject to pre -analysis, relevant cases for operational analysis are selected.

Conducting an in-depth analysis on every disclosure when the volume of reports exceeds the possibilities of the FIU to process them is not only inefficient, but also can lead to crucial information not being disseminated to competent authorities in a timely manner, jeopardizing the opportunities to tackle money laundering, associated predicate offences and terrorist financing crimes. The high volume of STRs/SARs received by the vast majority of FIUs makes it crucially necessary to develop efficient procedure, also supported by tailored IT tools, to select relevant cases and information that should be timely disseminated to competent authorities.

2.6 Conclusions and challenges on the FIUs' capacity to focus on relevant cases

Several FIUs have indicated various challenges associated with performing operational analysis. In particular, the two most frequently identified challenges are the steady increase of disclosures from reporting entities and the necessity for financial intelligence units to obtain sophisticated IT systems dedicated to the task of analysis.

The need to conduct the operational analysis on an increasing number of STRs put severe strains on financial, technical and human resources, as recalled in Chapter 1. A key role in this context is played by the capacity of FIUs, in line with international standard, to select relevant cases in order to handle the volume of disclosures received from reporting entities. Pre- analysis procedures developed by several FIUs (see paragraph above) may support this selection, but to face an increasing volume of disclosures there is also an increasing need for dedicated IT tools. The

interpretative note to FATF recommendation 29 also highlights the vital role of IT software in FIU analysis: "*FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links"*.

The use of dedicated IT tools has been highlighted by EU FIUs both in the process of selecting relevant cases for operational analysis and in the task of connecting information obtained from different sources. As already highlighted in Chapter 1, several units have designed in house IT systems to assist in operational analysis. Other FIUs have purchased commercial software from external providers (such as GoAML) and tailored these tools to their unique requirements. Nevertheless, many units have indicated a need to upgrade their existing IT systems, which may signal, that these solutions are reaching their full capacity.

Qualified personnel was also indicated as a challenge in conducting operational analysis. As mentioned earlier, the average number of human resources available to EU FIUs is 58 staff members. However, it must be taken into account, that 21 FIUs have less personnel than the aforementioned average and that the majority of FIU staff may be dedicated to other tasks than operational analysis (see on these aspects Chapter 1).

3. Results of operational analysis. Intelligence products suitable for use in investigations

All FIUs participating in the survey declared that the analysis they carry out specifically aims to develop intelligence products suitable for use in investigations. Consideration is primarily given to the types, functions and objectives of the authorities, to whom FIUs can disseminate information and, based on these elements, on what is included in the dissemination data (see also section 5.3 -Dissemination).

> STR/SARs are complemented, based on analysis, by technical reports prepared by the FIU. The technical report outlines the outcomes of the analysis and highlights possible leads for further intelligence and analysis. The STR and the technical report are accompanied by all relevant information gathered through the analytical process. The whole intelligence package, which is disseminated, adequately supports the ensuing investigations or prosecutions
>
> The FIU proceeds to filter and convert into qualified information the data at its disposal, for the purpose of providing a final product, which supports the following processes of the investigation bodies and judicial authorities.

The main recipients of intelligence products are the Police, public prosecutors, intelligence services, national security agencies and counter-terrorism authorities. As regards the content of intelligence products, one FIU reports that it disseminates two types of intelligence outputs: short reports relating to single transactions, or more detailed and thorough reports relating to a complex transaction scheme involving multiple parties, the latter being most useful to LEAs. Another respondent FIU has provided a further example of an intelligence product which can be developed by the unit.

> "The FIU's analysis can also lead to a Prohibition of Disposal of Property (PDP). The suspected predicate offence determines if a prosecutor should be consulted to approve or suspend the PDP. When the PDP is approved, an operative report is written and used in investigation".

The information provided through dissemination is in the vast majority of cases the basis for the initiation of preliminary investigations and criminal proceedings. A critical element is the potential use of the disseminated information as evidence in judicial proceedings. Three FIUs have explicitly

underlined that the information provided cannot be used in judicial proceedings. One FIU has informed that is can disseminate two different types of reports, with only one of them available for use as evidence.

The FIU can provide intelligence reports that can be used in investigations as starting point or directional information. Also, the FIU can provide official police reports that can be used as evidence in criminal investigations.

The responses provided indicate that EU FIUs forward to their competent authorities a variety of different intelligence products. Many FIUs have unique solutions regarding what information can be provided in the disclosures, who can be the recipient and how the information can be further used (for more on this issue see paragraphs … on the dissemination function). The capability of the FIU to provide good quality intelligence products to the appropriate authorities is directly connected with the powers related to conducting operational analysis.

This means, that differences affecting the way FIUs conduct operational analysis – in particular concerning available information sources available and the tendency for some law enforcement and judicial FIUs to integrate analysis with investigation – have an impact on the quality and usefulness of the final product provided to competent authorities. For example, the lack of access of the FIU to law enforcement information, especially concerning ongoing investigations and prosecutions, can result in a situation, where the FIU decides not to disseminate information which could be relevant for ongoing criminal proceedings. The tendency to connect analysis with law enforcement activities may on the other hand limit the possibility of the FIU to disseminate information to competent authorities other than those possessing a law enforcement/judicial status.

Furthermore the timeliness and quality of feedback received by the recipient authorities of intelligence products is crucial as it allows the FIU to better evaluate the findings of the financial analysis performed in the light of the subsequent investigations. This also plays a vital role in the possibility for the FIU to tailor the disclosures provided to the specific needs of competent authorities, and to be able to promptly integrate the disseminated information with additional information and data, where necessary.

4. Strategic Analysis

All but one of the FIUs participating in the survey indicated that they conduct strategic analysis. The remaining unit informed, that strategic analysis will be part of the NRA program, and that is meant to take place in the coming months.

In line with international standards and EU provisions, responses highlight that strategic analysis assist FIUs in identifying areas which deserve particular attention, so that the analytical efforts and available resources can be properly and efficiently deployed. In addition, FIUs strategic analysis provides insights into existing or prospective threats, essential for developing and updating the national risk assessment (see article 7 of the Directive).

The FIU conducts strategic analysis to detect and assess relevant trends and patterns and to identify weaknesses in the system. Strategic analysis helps in the orientation of the Unit's activities, the planning of initiatives and the prioritization of objectives (…). An additional purpose of strategic analysis is assessment of risk for the system as a whole or for selected geographical areas, means of payment and economic sectors. Defining risk levels enables the FIU to develop its own vision of the threats to and the vulnerabilities of the country's provisions against money laundering (…). By picking out situations and contexts that warrant closer analysis, strategic analysis enables the FIU

to prioritize its activities.

Strategic analysis should be based on various information sources. The *Operational Guidance for FIU Activities and the Exchange of Information* published by the Egmont Group highlights possible components of such an analysis:

- *examining data for patterns and similar concepts;*
- *developing a working hypothesis that addresses the "who", "what", "when", "where", "how", and "why" of the activity;*
- *collecting, evaluating and collating further information as required;*
- *identifying connections or links between pieces of information, also used to support an inference;*
- *developing inferences (an inference is the best estimate of the truth that can be drawn from facts, opinions or other inferences);*
- *constructing the argument, that is the logical flow of elements leading to the inference*

Respondents have also highlighted that STR/SAR and other disclosures received (i.e. threshold-based disclosures) are the main sources of data for strategic analysis. Relevant information may be also provided by competent authorities or taken from typologies reports developed by international organizations (i.e. FATF, Egmont Group) as well as from publicly available data.

Strategic analysis uses the information available, enriching it with input from external sources, both open and confidential. It rests on two pillars: the identification of the typologies and patterns of anomalous financial conducts and the observation and study of financial flows and money laundering.

FIU is able to analyse trends and patterns by evaluating information from STRs with regard to bank transfers, payments to other countries, currency exchange, cash withdrawals, as well as the nature of the industries that generate STRs. The purpose of this is inter alia to identify indications of typical predicate offences, i.e. the type of crime that is likely to yield proceeds. The information is presented in FIU's annual report with statistics over the number of STRs, the reasons for suspicion, national and international geographic spread, external requests, transaction methods and distribution over industries. The annual report functions as a summary of operations during the previous year. Apart from the annual report, strategic analyses are developed when there is a need or on request from another authority within the AML field.

Among EU FIUs there is a great variety of end products that are originated through strategic analysis. Money laundering and terrorist financing patterns and trends are developed and in some instances the results of strategic analysis are shared with relevant stakeholders through annual and periodic reports. Some FIUs take part in wider analyses conducted by the organization, in which they are embedded or conduct trend analysis for other LEAs. Many units contribute, through strategic analysis, to the national risk assessments.

The FIU develops strategic assessments of its own in relation to sectorial reporting and trend analysis for partner law enforcement agencies. The FIU also contributes to wider strategic analysis and reporting by others within the NCA in respect of what the SARs that we have received describe to us against national threats.

At least three respondents to the Survey have informed that a special unit within the FIU is dedicated to conducting strategic analysis.

The FIU has a strategic analysis unit staffed with three people. It is in charge of identifying and assessing new trends and schemes regarding money laundering and terrorism financing risks:
(i) through transversal processing of internal data and STR received by the FIU (countries targeted by international financial sanctions, non cooperative territories…)
(ii) or through active monitoring on emerging issues, in partnership with other relevant public or private entities (virtual currencies, new money services businesses…).

The unit in charge of strategic analysis contributes to the implementation of a risk based approach (…) following FATF Recommendation 1 and INR 1.

The FIU conducts strategic analysis, using available (e.g. STRs, CTRs) and obtainable information (e.g. from obliged entities) to identify money laundering and terrorist financing trends and patterns and produces annual and periodical reports available to the [FIU] management and employees (internally) and to the different sectors of reporting entities or general public, depending on the nature and the content of the report.

Three FIUs have also highlighted challenges regarding this type of analysis. All of these units pointed out the need for appropriate software or databases, to efficiently provide information necessary to discover patterns and trends. Differently from operational analysis, the main function of these IT systems should be focused on the possibility to select and identify patterns and trends from the information already received and gathered and disseminated by the FIU.

4.1 Conclusions and challenges on strategic analysis

The overview of the information provided by respondents clearly indicates that FIUs significantly differ in the way they conduct strategic analysis. EU FIUs aim towards the main goal of strategic analysis, that is the identification of trends and patterns in support of more focused action by the FIU or other competent authorities. Nevertheless, differences are visible, especially regarding the information sources available for strategic analysis and the use of the outcomes. As a consequence, FIUs appear to have varied capacities to perform strategic analysis and, based on this, exploit its full potential to support their own functions and properly contribute to the AML/CFT policies of other national competent authorities.

The introduction of strategic analysis as a mandatory task for FIUs in the Directive has created an obligation for all EU FIUs to develop a procedure to conduct strategic analysis and dedicate necessary resources to fulfill this task. The broader use of strategic analysis in the upcoming years will allow European units to be able to react more effectively to the constantly evolving patterns and trends regarding money laundering and terrorist financing.

As money laundering and terrorist financing trends and patterns have frequently a cross-border dimension, strategic analysis should not be merely restricted to the identification of trends and patterns in a particular country, as it seems to be done so far by most of the EU FIUs. It is worth noting that the Directive has introduced a supranational approach to the assessment of risks with a cross-border nature (see article 6 of the Directive), thus favoring an expansion of the horizon also of strategic analysis conducted by the FIUs.

Any vulnerability and gap in properly addressing the “supra national dimension” of ML and TF schemes through an effective exchange of information between EU FIUs can be exploited by criminal activities in a context characterized by strongly integrated markets and instruments. Therefore, EU FIUs should develop their cooperation towards identifying money laundering and

terrorist financing schemes with significant cross-border dimensions and develop strategic analysis products also through joint analysis of relevant phenomena. The said cooperation could also be helpful to improve the quality of national risk assessment, favoring the removal of possible inconsistencies in the risk assessment conducted by the different Member States and increasing their effectiveness in their capacity to identify and combat emerging threats.

The EU-FIU Platform can serve as a forum for such initiatives, as highlighted under article 51 of the Directive, which specifically foresees that, through the EU FIUs' Platform, FIUs should work for *the identification of trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level*. Also the introduction of cross border report regime, pursuant to article 53(1) could favor the detection of trends in the patterns of criminal activities with a cross border dimension and the sharing of information also of strategic nature through joint analysis.

5. Dissemination to competent authorities (spontaneous)

The characteristics of the dissemination functions, both spontaneous and on request by domestic competent authorities, have been recalled in Chapter 2 (paragraph 2.3), where the independence requirements associated with these functions have been discussed. This Chapter focuses specifically on the FIUs' capacity to perform the dissemination function by ensuring that the cases and the information disseminated are selected in a manner that allows recipient agencies to properly focus their action and use their resources efficiently.

5.1 Capacity to select the cases to disseminate

Pursuant to article 32(3) of the fourth Directive, consistently with the features of the analysis function, also dissemination has to be performed by FIUs under a selective approach. As discussed above in relation to the analysis, while all information received or otherwise available to FIUs have to be considered, relevant cases potentially indicative of money laundering or terrorist financing offences, should be identified. Similarly, when it comes to dissemination FIUs should forward to competent authorities relevant information which, in turn, allows law enforcement agencies to focus on priority and develop targeted and effective action.

With one exception, all the FIUs responded that they have the capacity to select the cases and the information for dissemination and to support the efforts of law enforcement authorities and assisting recipient authorities to focus on relevant cases.

5.2 Capacity to select the information to disseminate; the recipient authorities

In relation to the capacity to select the information to disseminate, only half of the respondents have indicated that they are able to disseminate specifically the results of their analyses, as opposed to forwarding the entire set of information received through disclosures and gathered in the course of the analyses.

The dissemination of all information received does not seem to be in line with the provisions of article 32(3) which stipulates that "(...) the FIU shall be responsible for disseminating the results of its analyses and any additional relevant information to the competent authorities where there are grounds to suspect money laundering, associated predicate offences or terrorist financing (...)".

The scope of "competent authorities" designated as recipient of the FIU's dissemination varies among different Member States; in some instances it includes also judicial authorities, supervisors

and fiscal authorities, besides law enforcement agencies. In several cases FIUs take determinations on which competent authorities should be recipient of each particular dissemination, depending on the nature and the expected follow up of the cases, while in other instances the recipients of dissemination are specifically designated by the law.

The following table provides an overview of the authorities that, in each Member State, receive the dissemination from the FIU. The information has been gathered primarily from responses to the Survey. In cases where these are not specific (as, for example, general reference is made to "competent agencies"), additional information has been taken from other sources, namely the latest Mutual Evaluation Report available for interested Country and the Report on "Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorism Financing Policy" ("ECOLEF"), 2013. It is important to underscore that this additional information may not be updated.

FIUs' dissemination – Recipient domestic authorities					
Member States	**LEAs**	**Judicial**	**Supervisory authorities**	**Tax authorities**	**Others**
Austria	• Regional or Federal police forces (also antiterrorism)	• Prosecutors		• Tax Administration	• Customs • Anti-Corruption
Belgium*	• Federal judicial police • Local police	• Prosecutors • Federal Prosecutor	• Financial Services and Markets Authority • National Bank of Belgium	• Anti-Fraud Co-ordination Service (CAF) at FPS Finance	• Customs • OLAF • National Social Security Office • Intelligence services
Bulgaria**	• Competent police forces[120]	• Prosecutors			
Croatia[121]	• Min. Int.-Police Directorate • Financial Police	• State Attorney Office	• Financial Services Supervision Agency • National Bank	• Financial Inspectorate • Tax Administration	• Customs • Security Intelligence Agency • Ministries
Cyprus	• Specialised police forces	• Prosecutors	• Sectoral supervisors	• Tax administration	• Customs
Czech Republic***	• Police Unit for Combating Corruption and Financial Crime	• Specialised Prosecutors		• Tax Administration	• Customs
Denmark**	• Police forces	• Office of Prosecution for Serious Economic Crimes	• Financial Services Authority	• Tax Authorities	• Danish Commerce and Companies Agency
Estonia**	• Police forces • National Security Police	• Prosecutors	• Financial Supervision Authority	• Tax Authorities	• Customs
Finland**	• National Bureau of Investigation • Security Police	• Prosecutors			

[120] The AML Law (article 12(4)) does not specify particular recipients for dissemination. The FIU provides the information to the prosecutor's office or to the relevant security and public order service based on its own decision.

[121] The AML Law (article 58) generally refers to dissemination to a "competent state body". This includes, i.a., the State Attorney's Office of the Republic of Croatia, the Ministry of the Interior – the Police Directorate, the supervisory services of the Ministry of Finance (the Financial Inspectorate, the Customs Administration, the Tax Administration and the Financial Police), the Croatian Financial Services Supervision Agency, the Croatian National Bank, the Security-Intelligence Agency, the Ministry of Foreign Affairs and European Integration, the Ministry of Justice and with other state bodies

France	• Police forces	• Regional and State Prosecutors		• Directorate General of Public Finances	• Intelligence Services • Customs • Social administrations
Germany	• Land Police Bodies			• Tax authorities**	• Specialised Terrorist Financing Unit of the BKA** • Customs investigation offices**
Greece**		• Prosecutors			
Hungary	• Police forces • Counter-Terrorism Center	• Prosecutors		• Tax and Customs Investigators**	• National Security Services
Ireland	• Police forces				
Italy	• Police forces				
Latvia**	• Police forces	• Prosecutors			
Lithuania	• Local police forces • State Security Department (TF cases)				
Luxembourg	• Police forces	• Prosecutors**			
Malta	• Police forces				
Netherlands**	• National Police • Royal Netherlands Marechausse • Special LEAs (ISZW; NVWA; Rijksrecherche; FIOD; ILT-IOD	• The National Prosecution's Office • Financial, environmental and food safety offences Prosecution Office		•	• National Security Services
Poland	• Police forces • Internal Security Agency • Other intelligence services	• Prosecutors	• Financial Supervision Authority	• Tax administration	• Customs • Border Guards
Portugal**	• Economic and Corruption Department	• Central Department for Investigation and Prosecution (DCIAP) • District Prosecutors		• Tax authority	
Romania	• Romanian Intelligence Service	• The General Prosecution's Office by the High Court of Cassation and Justice			
Slovak Republic	• Police forces	• Prosecutors		• Tax Directorate	• Customs Directorate

Slovenia	• Police forces	• Prosecutors		• Tax Office**	
Spain**	• National Police (CNP) • Civil Guard	• The National Court Prosecution Service • The Anti-drugs Prosecution Service • The Anti-corruption Prosecution Service		• Tax Agency	• Customs authorities • Other government bodies
Sweden**	• Economic Crimes Bureau • National Police • County Police	• Swedish National Prosecution Authority		• Economic Crimes Unit of the Swedish Tax Authority	• Customs Service • National Security Service
United Kingdom**	• Police Forces • Serious Fraud Office	• Crown Prosecution Services			• Her Majesty's Revenue and Customs

* Source: FATF, Mutual Evaluation Report, 2015
** Source: ECOLEF Report
*** Source: MONEYVAL, Mutual Evaluation Report, 2011

Taking into account the widening scope of disseminated information, which now expressly makes reference also to the ground to suspect "associated predicate offences" further analysis could be developed on the consequences, particularly on effectiveness, of the discretion granted to the EU FIUs in identifying the authorities that should receive their spontaneous disseminations. From a general perspective the possibility to identify –according to the results of the analysis- the most appropriate recipient of the spontaneous dissemination would seem to ensure that the information is provided more timely where needed.

Further details may be collected to understand existing coordination mechanisms in place to avoid possible overlapping of competences where more recipients are involved and to have a clearer understanding of the criteria applied to identify the recipients.

In terms of effectiveness it should also be considered that the capacity of the FIUs to select the information received is intrinsically affected by the timeliness and quality of the feedback received by the recipient authorities. In this perspective, paragraphs 3 and 4 of article 32 of the Directive, about the FIU's dissemination, should be read, and implemented, in conjunction with the following paragraph 6 which requires competent authorities to provide feedback to the FIU about the use made of the information provided and about the outcome of the investigations or inspections performed on the basis of that information.

A tailored analysis on the dissemination capabilities of EU FIUs could be helpful to shed more light on national practices, with a view to identifying those that could be shared, particularly on the following aspects:

- the range of authorities to which the information available to FIUs is disseminated, also in light of the consideration of the underlying "associated predicate offences" for money laundering cases;
- tailored outputs and products produced by FIUs taking account of different cases and the selected recipients;
- mechanisms set up to ensure that the intelligence products are aligned with the operational need of the recipient authorities;
- dissemination mechanisms and communication channels;
- security and confidentiality issues related to the disseminated flows of information;
- feedback mechanisms on the use of disseminated information.

6. Capacity to provide information on request from competent authorities (dissemination on request)

Through dissemination FIUs support the efforts of the competent authorities providing new triggers for investigations as well as financial intelligence related to cases that are already under investigations. A smooth and comprehensive cooperation between FIUs and law enforcement authorities is therefore vital to the good functioning of the AML CFT framework in this respect.

FIUs can disseminate information both spontaneously, as results of the financial analyses or at request of the competent authorities, where dissemination mainly support ongoing investigations money laundering, associated predicate offences or terrorism financing. Differently from the spontaneous form, dissemination on request is not compulsory for FIUs, which maintain a certain

level of discretion. Moreover, the Directive explicitly foresees a number of cases where FIUs can decline requests for STR/SAR information by domestic competent authorities[122].

Several respondents have pointed out that they face no particular legal constraints with regard to dissemination of information to other authorities. Only one FIU indicated that it does not have the capacity to provide STR/SAR information upon request of domestic competent authorities. Several differences have been reported as regards the "competent authorities" to which the FIU can forward STR/SAR information upon request from the latter. For the majority of respondents, these authorities include law enforcement and judicial agencies; some FIUs have indicated that, in addition, they can provide information to supervisory authorities or to fiscal bodies.

It has to be underlined that the discretional nature of the FIUs' dissemination on request, together with the explicit identification of cases in the Directive (although in general terms, with potentially diverging interpretations across Member States) where the request for dissemination can be refused, are in line with, and provide further confirmation to, the status of autonomy and operational independence of FIUs: these cannot be forced to disseminate information beyond what follows naturally from the outcome of their analysis as a core function in support to ensuing investigations.

In the same perspective, as well as to allow FIUs to exercise their discretion in a proper and informed manner, it is important that requests for dissemination are duly motivated, clearly explaining the context and purposes for which the information is sought, so that the relevance of the required disclosure with regard to the purposes for which it has been requested can be adequately considered.

For the same reasons related to the FIUs' status of independence, beyond the spontaneous dissemination and the dissemination on request other forms of access to STR/SAR information should not be possible for domestic authorities. In this respect, it is important to recall the concerns raised in Chapter 2 on forms of direct access to, or sharing of, FIUs' information with other domestic agencies, mentioned by respondents[123].

7. Postponement of suspicious transactions

7.1 Capacity to postpone

Article 32(7) of the Directive makes reference to the power of the FIU to 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, in order to analyze the transaction, confirm the suspicion and disseminate the results of the analysis to the competent authorities.

While the majority of EU FIUs have confirmed that they have the capacity to postpone suspicious transactions, others have flagged that they still lack this power which is expected to be introduced following the implementation of the fourth Directive.

[122] Article 32(5) of the Directive references "objective grounds for assuming that the provision of such information would have a negative impact on ongoing investigations or analyses" and "exceptional circumstances, where disclosure of the information would be clearly disproportionate to the legitimate interests of a natural or legal person or irrelevant with regard to the purposes for which it has been requested".

[123] See also the concerns expressed in the same Chapter on forms of multiple reporting of STRs/SARs to the FIU and to other authorities.

The lack of powers to postpone a transaction (besides contrasting with the provisions in the Directive) can jeopardise the capacity to promptly restrain criminal funds or assets, also for seizure purposes.

7.2 Duration of postponement

The duration of the FIUs' postponement varies greatly across EU FIUs. It ranges from two days till an unlimited time. The information provided in this regard by respondents are outlined in the following table; the data should however be considered with some caution as the starting point for the postponement can be differently considered under the relevant legislation of EU Member States.

FIU	Duration of the postponement
Austria	**6 months**
Belgium	**5 working days**
Croatia	**72 hours**
Cyprus	**No maximum duration**.
Czech Rep.	**72 hours**
Denmark	**For up to one week** or **permanently**.
Estonia	**30 + 60 days**
Finland	**5 working days**
FIU Bulgaria	**Up to 3 business days**.
France	**5 days**
Greece	**Until the court reaches a final decision**.
Hungary	**5/7 working days**.
Italy	**5 working days**
Latvia	**50 days** or **125 days**. or up to **6 months**.
Lithuania	**10 working days**.
Luxembourg	**6 months** (**3 months that may be extended 3 times by 1 month**)
Malta	**3 working days**.
Poland	**3 days (FIU) extended to a definite period up to 3 months (prosecutor)**
Portugal	**2 working days**
Romania	**48 hours** + **other 72 hours**
Slovenia	**72 hours**
SVK	**120 hours** (FIU) + **additional 72 hours** (LEA)
Sweden	**2 working days**.
United Kingdom	**seven working days** + **further 31 calendar days**

Taking into account the cross-border nature that criminal financial activities frequently assume, and the need to ensure that suspicious transactions can be postponed effectively also in the context of FIU-to-FIU cooperation, significantly diverging durations of FIUs' postponement orders can have detrimental effects on FIUs' action and cooperation in these contexts. More uniform approaches would benefit the overall capacity to stop and seize criminal funds in cross-border situations.

The need for more uniformity in the postponement function should be emphasized also in light of the new obligation for FIUs to forward cross-border reports to interested counterparts (article 53(1) of the Directive, also to allow joint analysis) and on the duty to postpone suspicious transactions also on behalf of foreign counterparts.

It also has to be considered that postponement is a delicate power to activate, as the reporting

entity is required to interact with the reported subject respecting also the tipping off prohibition. Therefore, any harmonized approach in this respect shall identify a proper balance between the need to preserve confidentiality and the need to set forth an adequate time allowing assess the case, with the FIU liaising with competent law enforcement agencies or prosecutors to establish if the postponement can be followed by seizure orders.

Moreover, taking into account the provisions in the Directive about the postponement on behalf of foreign FIUs a harmonized ad hoc procedure for postponement seems all the more needed to ensure that a prompt action and feedback can be ensured in cross-border situations.

For the same reasons, more targeted provisions concerning the exemption of liability and the physical protection of involved staff, both from the reporting entities and from the FIUs involved, may be needed to facilitate the correct implementation of postponement powers, both domestically and in the context of FIU-to-FIU cooperation.

7.3 Procedure

The Directive (Article 35) establishes that "Member States shall require obliged entities to refrain from carrying out transactions which they know or suspect to be related to proceeds of criminal activity or to terrorist financing until they have completed the necessary action in accordance with point (a) of the first subparagraph of Article 33(1) and have complied with any further specific instructions from the FIU or the competent authorities in accordance with the law of the relevant Member State". The exception to this rule is where refraining from carrying out transactions is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected operation. In this exception, the obliged entities concerned must inform the FIU immediately afterwards.

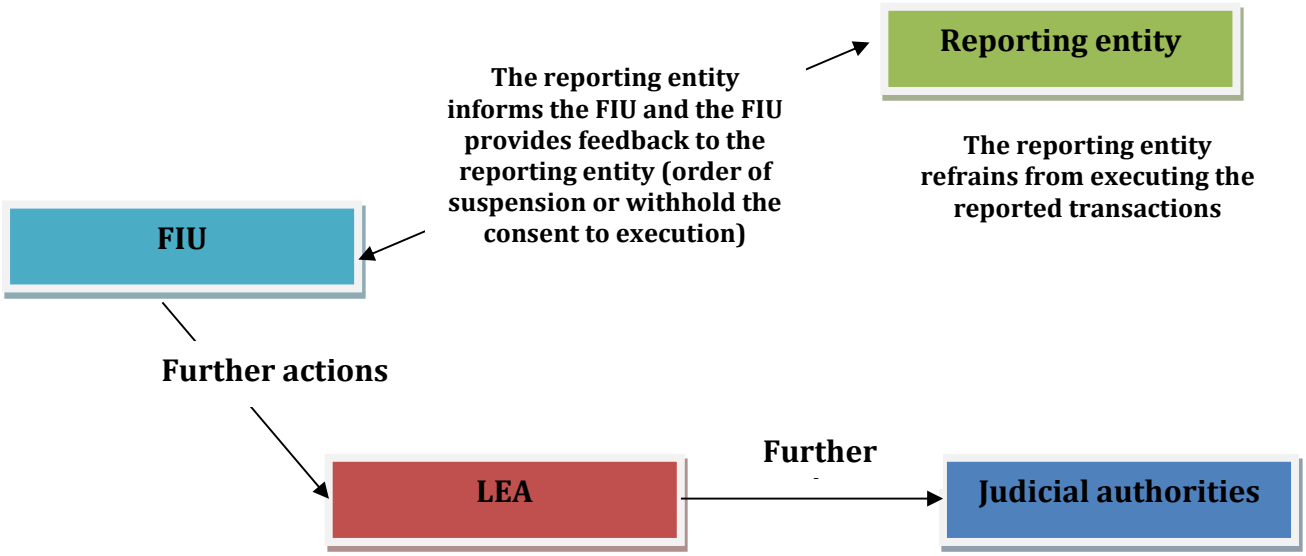
Once the decision to suspend the transaction has been taken it is pivotal that further action and the necessary liaison of the FIUs with competent authorities are taken as quickly as possible, so that the reporting entity receives an immediate and a prompt feedback from the FIU.

The different mechanisms of direct suspension and of withdrawal of consent to the transaction to go ahead should be briefly recalled and described.

A respondent to the Survey has indicated that all consent requests are treated as a priority within the FIU. As soon as a decision is made it is relayed to the reporter without delay. The FIU is required to reach a decision within strict timescales set down in legislation. The law specifies that consent decisions must be made within seven working days from the day after receipt of the consent request (excluding bank holidays and weekends). If consent is refused within the seven working days, law enforcement has a further 31 calendar days – from the day of refusal – to further the investigation and take further action e.g. restrain or seize funds. The 31 days includes weekends and bank holidays.

Under the anti-terrorism law, the statutory timescale is seven working days from the day after receipt of the request to provide a response. In contrast to the consent under the AML legislation, once a request is refused there is no moratorium period for recovering the property or for subsequently granting consent, though there is a duty to keep the decision under review in light of a change in circumstances and further information received.

While the duration of postponement varies across Member States, the procedure generally follows the pattern described below:



Deviations from this general scheme are also found. For example, a respondent to the Survey informs that, while the suspension is initiated and proposed by the FIU, the order executing the postponement is issued by the Minister of Finance.

The Director of the FIU initiates the process for postponement of a transaction, but it is formally the Minister of Finance who issues the postponement order. According to the [AML Law], in cases provided for in Art. 11 and 18 (STR submitted or request from foreign FIU received), the Minister of Finance may, upon a proposal by the Chairperson of FIU, postpone, by a written order a certain transaction or deal for a period of up to three business days. The FIU shall notify the Prosecutor's Office immediately about the postponement of the transaction, providing relevant information thereto. The prosecutor may impose a preventive measure or file a request with the relevant court to impose an impoundment or injunction.

Another respondent highlights that, based on domestic law, the FIU is obliged to inform of the postponement the customer involved. The customer, in fact, has the possibility to file a complaint with the Federal Administrative Court for violations of his/her rights.

The FIU is empowered to order that an ongoing or upcoming transaction with respect to which there is suspicion or reason to suspect that the transaction serves the purpose of money laundering (...) or terrorist financing be omitted or delayed temporarily and that customer instructions involving outgoing funds only be executed with the consent of the FIU. The FIU must inform the customer and the public prosecutor's office of this instruction without unnecessary delay. The notification to the customer must include an indication that the customer or another party concerned is entitled to lodge a complaint with the Federal Administrative Court regarding violations of their rights. (3a) The FIU must reverse the instruction pursuant to para. 3 as soon as the conditions for its issue are no longer fulfilled or the public prosecutor declares that the conditions for confiscation (...) are not fulfilled. Otherwise, the instruction is to be abrogated: 1. once six months have elapsed since it was issued; 2. as soon as the court has issued a legally effective decision on a request for confiscation (...).

This mechanism of notification raises of course issues of tipping off and lack of confidentiality (both as regards the postponement and the existence of the underlying suspicious transaction report), together with concerns related to the exposure of the reporting entity and its staff (but also of the staff of the FIU).

The variety of mechanisms (order for suspension, withholding of the consent for the transaction to go ahead) and procedures in place, with instances of involvement of third parties or of information being provided to the reported customers, highlights the need of more detailed provisions or guidance. More specifically, issues to tackle include how suspicious transactions should be treated in the reporting procedure, particularly as regards the obligation for the reporting entity to refrain from execution, the relations with the subjects involved in the suspicious transactions put on hold, the FIUs' actions for postponing and communicating with the reporting entities and with law enforcement agencies.

8. Conclusions

The vast majority of EU FIUs declared that they conduct both operational and strategic analysis as foreseen by article 32(8) of the Directive. Based on the responses to the Survey, FIUs consider themselves in line with the provisions in the Directive and in international standards on these core functions. Nevertheless, the vagueness surrounding the distinctive features of "analysis", in lack of a common definition or description, entails that in some instances FIUs' analytical function are not carried out as a different and separate activity with respect to investigation, aimed at adding value to the information received to support the latter. Together with differences in domestic activities carried by FIUs, diverging understandings on what "analysis" is and approaches to what it entails and how it should be carried out are at the basis of significant "mismatching" in expectations by FIUs when it comes to providing and receiving cooperation.

EU FIUs have provided different responses concerning the scope of "operational analysis", namely as to whether they analyze each received STR/SAR or if they focus on selected cases. Several responses indicate, that although EU FIUs take into account all disclosures received, the majority of respondents conduct an initial pre-analysis on all transmitted STRs in order to select relevant information for further operational analysis.

Taking into account the increasing volume of disclosures received from reporting entities the capacity of FIUs to be "selective", throughout their analysis up until the dissemination of its outcome becomes crucial both to ensure an adequate treatment to disclosures according to priorities and to allow law enforcement agencies to focus on substantiated money laundering or terrorist financing cases.

Coupled with the lack of a common notion of STRs/SARs, which, as seen, vary considerably across Member States in volumes, structure and content[124], the lack of a common notion of "analysis" may enhance the differences in national approaches taken by Member States and FIUs to pursue the objective of tackling increasing volumes of disclosures and information, by at the same time considering all relevant information and ensuring an adequate selection of cases, so that resources available to the FIUs themselves and to partner law enforcement agencies can be used efficiently. Together with domestic effectiveness, differences among FIUs in the analytical activities carried out and in the ways in which cases and information are prioritized and selected may well affect also the capacity to entertain adequate FIU-to-FIU cooperation.

[124] See Chapter 3.

Taking into account the highlighted issues regarding operational analysis, provisions or guidance at the EU level on the nature and features of "analysis" as a core and independent FIUs' function may bring considerable benefits to both effective domestic activities (which in turn could better support money laundering and terrorist financing investigations and prosecutions) and to FIU-to-FIU cooperation.

Results of FIU operational analysis are provided to competent law enforcement authorities in the form of ad-hoc intelligence products. All EU FIUs have indicated that these products are suitable for the use in investigation. In any case, the types and quality of the outcomes forwarded to law enforcement agencies is directly dependent on the type of the underlying analysis: as this latter differ considerably, so do the former. As a result, the content and format of the intelligence disseminated by EU FIUs is also varied. Differences have also been highlighted as to the purposes that disseminated products are intended to serve; on this point, responses highlight that the intelligence elaborated by FIUs is mostly meant to assist police bodies and prosecutors to develop their own investigations, while in some cases this intelligence can also be used as evidence in the context of legal proceedings.

It is also important to underscore the crucial relevance of feedback from competent authorities to the FIU on the use of the disseminated information and on the outcome of the investigations performed on the basis of that information, as required under article 32(6) of the Directive. This feedback allows the FIU to focus its analysis on relevant cases and phenomena, taking account of the evolving experience, and to constantly adjust its intelligence products to the needs and expectations of end users.

Nearly all FIUs conduct strategic analysis. The respondents have provided indications on information sources for strategic analysis and on the recipients of the related outputs. In several instances, responses also confirm that data gained through strategic analysis is also used in the national risk assessments as well as in broader research activities conducted by the institution in which the FIU is embedded.

Although almost all EU FIUs conduct strategic analysis, significant difference can be observed in its features and final use. Due to cross-border dimension of money laundering and terrorist financing, consideration has to be given to enhance cooperation between EU – FIUs in the field of conducting strategic analysis in order to assess ML/TF trends and patterns more comprehensively.

The EU-FIU Platform can serve as a forum for such initiatives, as highlighted under article 51 of the Directive, which specifically foresees that, through the EU FIUs' Platform, FIUs should work for the identification of trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level.

It is important to highlight that several FIUs have indicated that they face challenges in carrying out their analysis functions. Concerns are mainly related to capabilities and effectiveness. In particular, respondents have underlined problems in coping with constantly increasing volumes of disclosures received; in some instances, these problems are aggravated by the lack of appropriate IT systems to assist them in performing this function. As mentioned earlier, when confronted with sizable numbers of STR/SARs, FIUs should have the capacity to be "selective" in order to focus on relevant cases. Sophisticated IT systems can significantly improve the process of selecting these cases and conducting operational analysis in general.

While the Directive does not specifically deal with the use of IT systems in support of FIUs' analytical functions, article 32(3) sets out an obligation for Member States to provide FIUs with

adequate financial, human and technical resources in order to fulfil their tasks. A more tailored approach on this issue is reflected in FATF standards, where Interpretive Note to Recommendation 29 specifically establishes that FIUs should be encouraged to use analytical software to process information more efficiently and assist in establishing relevant links.

Against this background, and in light of the increasing workload and volumes of disclosures and information that FIUs have to process, at the same time ensuring rapidity (e.g. for adequate prevention in terrorist financing-related cases or for acting in cases of postponement), effectiveness and selection of relevant cases, common provisions at the EU level might be appropriate to encourage Member States and FIUs to develop IT resources in support of analytical functions.

In relation to the provision of the Directive according to which "the FIU shall be responsible for disseminating the results of its analyses and any additional relevant information", it has to be taken into consideration the fact that the majority of respondents to the Survey have indicated that they only forward to competent law enforcement agencies the results of the analyses (apparently without "additional information" gathered in the course of the analysis). It is important that, as the final goal is to mitigate risks of money laundering and terrorism financing and identify actual cases of criminality in these areas, FIUs be able to provide to competent authorities any additional relevant information available, in accordance with their needs.

As regards the FIUs' dissemination, responses seem to highlight significant differences across national approaches, particularly for what concern the types and scope of the intelligence provided and the "competent authorities" designated as recipients. These authorities include, in few instances, also judicial, supervisory or fiscal authorities. On this point, a more targeted overview may provide helpful insights on existing practices, which could be shared to foster convergence, and a more in-depth understanding of EU FIUs' dissemination systems. This may also facilitate international cooperation, particularly as regards the provision of the consent to forward the information shared to other domestic agencies (as these agencies would generally be known in advance to the requested FIU).

On the FIUs' capacity to postpone suspicious transactions, while the majority of the respondents have confirmed that this is in place in line with the requirements in the Directive, there are still several FIUs whose Member States, based on responses, have not yet introduced the necessary implementing legislation. Furthermore, existing postponement regimes feature several different approaches; for example, the duration of the suspension varies considerably across Member States, causing potential difficulties for the postponement of suspicious activities that have a cross-border nature through FIU-to-FIU cooperation. Differences exist also in the applicable procedures (with risks of tipping-off and lack of confidentiality) and in the subjects involved. More detailed provisions at the EU level would seem necessary to tackle these issues by ensuring more uniform and convergent approaches by FIUs, which would in turn foster effectiveness and facilitate cooperation.

CHAPTER 6

COOPERATION WITH OTHER FIUs

1. General aspects

1.1 Capacity to exchange information

The capacity to exchange information with foreign counterparts is widespread across all EU FIUs. All respondents have confirmed that they are able to provide information to their EU counterparts and, more broadly, to FIUs from other countries, based on adequate domestic legal bases. Responses also stress that the exchanges are performed generally in a timely and comprehensive manner and include information available or obtainable. Requests are constantly monitored by the receiving FIUs, to determine the level of priority and the information needs, and basically all responded. Limitations are reported in relation to resource constraints, which may limit the capacity to deal with all incoming requests with the appropriate priority, the need to obtain authorisations for accessing and sharing certain information, the frequent lack, in the requests, of adequate indications about the case and the links with the country of the requested FIU.

In several cases, the scope of the foreign FIUs that are "eligible" as counterparts for the exchange is universal, simply based on the recognition that they qualify as "FIUs" based on domestic laws and in accordance with the definition provided for in international standards. In some cases, the capacity to cooperate is limited to the FIUs that have been accepted as members of the Egmont Group. Membership of the Egmont Group is particularly broad and in fact entails a recognition that the definition of "FIU" is met.

This exchange, for all respondents to the Survey, can be either upon request from other FIUs seeking information or spontaneous, whenever the providing FIU believes that information available to it can be of use to a counterpart (due to, for example, links with the country of the latter or with a case dealt with in previous exchanges).

In accordance with the provisions of the fourth Directive, which on this point confirms the previous third Directive along a line of development which dates back to the Council Decision 2000/642/JHA and mirrors the international standards of the FATF and of the Egmont Group, the EU FIUs' capacity to exchange information serves, and is dependent upon, a specific purpose which defines its scope: information can (only) be shared "for the processing or analysis of information related to money laundering or terrorist financing and the natural or legal persons involved" (article 53(1) of the fourth Directive).

1.1 Purpose limitation: exchange for FIUs' analytical purposes

Based on the purpose limitation which defines the scope of FIUs' operations, FIU-to-FIU cooperation is exclusively aimed at facilitating the FIUs' typical function of analysis of suspicions, an activity which is well distinct and separate from investigation and prosecution on the same facts (performed by law enforcement bodies and prosecutors)[125]. Information exchanged between FIUs, therefore, is not destined to be used in the context of investigations, prosecutions or legal proceedings[126].

This remains true also when the FIU, having a police or judicial status, is also in charge of law enforcement activities, in addition to the functions associated with receipt and analysis of STRs/SARs. In fact, the purpose limitation of FIUs' cooperation as a tool in support of FIUs' analytical activities applies regardless of the nature or status of the FIUs, be they administrative, law enforcement, judicial or hybrid. Due to the purpose limitation, the receiving FIU can neither use the information exchanged for law enforcement purposes not forward it to police agencies or prosecutors for the same purposes, at least not without the prior consent of the foreign counterpart.

It is important to recall that, based on EU provisions in the fourth Directive, all FIUs perform analysis on suspicious money laundering or terrorist financing cases, different from investigations or prosecutions, and cooperate among themselves by exchanging information for this purpose, regardless of their nature or status. Equally, information exchanged between FIUs for analytical purposes cannot be used for pursuing other activities of which the receiving FIU may be in charge, such as supervisory tasks on the compliance with AML/CFT obligations.

As the purpose of FIUs' cooperation is focussed on allowing analyses on suspicious cases, the information exchanged cannot be used as evidentiary material in legal proceedings. In fact, while the analytical intelligence shared among FIUs may well assist competent authorities in identifying relevant investigative leads and can trigger Mutual Legal Assistance Requests (MLAR), any use of the information beyond its original purpose, as well as its dissemination to other parties, requires a prior consent by the foreign providing FIU.

Responses to the survey confirm that EU FIUs conform to this requirement. FIUs that have a police or judicial status have indicated that they can exchange information with EU counterparts as a separate and autonomous activity with respect to the cooperation carried out, for different purposes, through law enforcement or judicial channels.

The necessary distinction between FIUs' analysis and law enforcement activities, and the confinement of the FIUs' action to the former in accordance with the purpose limitation established in article 53(1), also entails that FIUs' analysis and the associated cooperation should be not only separate but also independent from law enforcement functions and criminal law considerations. More specifically, while FIUs should limit themselves to cooperating and exchanging information for analytical purposes, this cooperation and exchange should not be limited or conditioned by law enforcement "concerns", even in the presence of investigations or legal proceedings on the same

[125] It is important to recall that the purpose limitation, which keeps the FIUs' analytical activities distinct and separate from law enforcement tasks, applies equally to FIU-to-FIU cooperation and to FIUs' domestic functions: while the former is covered, as mentioned, by article 53(1) of the Directive, article 32(3) clearly envisages that FIUs are in charge of, i.a., "analysis" as a peculiar function distinct from others, such as investigation. This point has also been mentioned and discussed in previous Chapters, under different perspectives (see particularly Chapter 5, on FIUs' domestic functions and Chapters 1 and 2 on organization and independence).

[126] This further use or dissemination is dependent on a specific agreement between the parties involved and is subject to a prior consent by the providing FIU: see, in this Chapter, paragraph 10.

case or subjects or by considerations on the actual existence or nature of particular crimes. In other words, FIUs, in fulfilling their duty of cooperation in accordance with article 53(1) of the Directive[127], should in all cases remain free (and required) to share information regardless of the existence of law enforcement activities and of the identification of underlying predicate offences[128].

Clearly, that FIU-to-FIU cooperation, as a distinct and independent area of activity, should not be conditioned by law enforcement concerns derives as much from the principle of purpose limitation, embedded in article 53(1) as from the requirement of operational autonomy and independence stated in article 32(3)[129].

Nonetheless, as will be discussed in paragraphs …, responses show that in some cases the capacity to provide cooperation to other FIUs in support of analytical tasks is impaired by the existence of investigations or prosecutions in the Country of the requested FIU and by the need to obtain prior authorisations from competent prosecutors (importantly, these limitations may apply equally to police and other types of FIUs). Responses also show that police FIUs are in general able to exercise their domestic powers to obtain information for responding to requests from other EU counterparts.

One respondent has indicated that the cooperation and the exchange of information with other EU FIUs, including through the exercise of domestic powers to obtain information, is not a separate function from law enforcement activities and cooperation that it carries out.

There are also cases reported where information (of a financial or law enforcement nature) cannot be exchanged among FIUs without either ad- hoc authorisations issued by competent prosecutors or requests filed through police international cooperation channels (see, for example, paragraphs 1.4 and 1.8 in this Chapter). These conditions apply particularly when investigations or legal proceedings are underway on the same cases.

The distinction between analysis and investigation is not always neatly drawn and these two tasks may not be separated in a sufficiently clear-cut manner in all cases, both as regards domestic FIUs' functions (see the considerations on this point in Chapter 5) and in the course of FIU-to-FIU cooperation. As a consequence, the capacity of FIUs to provide cooperation in support of analysis, in line with the purpose limitation set out by the Directive, may be unduly constrained by concerns and conditions stemming from considerations pertaining to the conduction of law enforcement activities and cooperation.

Conditions limiting the information sharing include: a) the indication and nature of predicate offences being pursued by the requesting counterpart; b) the existence of investigations or legal proceedings on the same case in the country of the requested FIU; c) the need to obtain

[127] The exchange information is in fact set as an unconditional obligation for FIUs: "Member States shall ensure that 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 and the natural or legal person involved". Very limited exceptions are mentioned in article 53(3) but none of them mentions that the exchange can be limited or refused due to the existence of investigations or legal proceedings.

[128] The seme principles and line of reasoning can of course be applied, beyond the initial exchange of information, to the consent to further use or disseminate that information for other purposes: this also has to be granted independently from law enforcement concerns. There may be however some particular restrictions in this respect, although certainly more limited that those identified in current practices and national laws (see the discussion in paragraph 10), particularly connected with the need not to hamper ongoing investigations or legal proceedings in the country of the requested FIU.

[129] "The FIU shall have the authority and capacity to carry out its functions freely, including the ability to take autonomous decisions to analyse, request and disseminate specific information".

authorisations to exchange information from law enforcement or judicial bodies. The existence of these conditions, and their impact on FIU-to-FIU cooperation, is confirmed by responses and will be discussed more amply in following paragraphs.

At the same time, due to a blurred distinction and a lack of a clear separation between analysis and investigation, FIUs that are in charge also of law enforcement tasks (possibly confounded with analysis and carried out in a conjoint manner) may use information obtained from foreign FIUs in this context too, with possible tensions with the purpose limitation stated in article 53(1) of the Directive. It is also important, in these cases, that the providing FIU is properly informed about the expected use of the information and agrees to it.

To address these issues and reaffirm the purpose limitation which lies at the basis of FIUs' analysis and cooperation, it is important to stress the need to maintain analytical activities and law enforcement tasks separate. The following points should be considered for appropriate action at the EU level, either through targeted provisions or guidance:

- the distinction between analysis and investigation, both as regards FIUs' domestic activities and their cooperation, should be reinforced and clarified;
- the purpose limitation should equally be confirmed and detailed in its implications, clarifying that information should be exchanged by FIUs regardless of law enforcement concerns and that the information exchanged is to be used by the receiving FIU exclusively for analysis[130].

1.3 Purpose limitation: exchange on money laundering or terrorist financing cases

Not only FIU-to-FIU exchange of information is carried out in support of analytical activities; it is also limited to analyses focussing on potential money laundering or terrorist financing cases. Several respondents have pointed out that they cannot share information beyond this scope, namely for pursuing cases that may be related to different forms of criminality. In some important cases, the indication of the type of illegal activity which is under analysis by the requesting FIU constitutes an essential element for the request to be processed and a condition for being able to provide cooperation: information can be shared only if the case relates to money laundering or terrorist financing and if this is demonstrated in the request.

Normally, general references are sufficient to fulfil this requirement, without a need for a detailed description of the crimes specifically involved (see specifically par. 2.3 for more details on how the type of the underlying criminality influences the capacity to provide information and allow for its further use or dissemination). It is important that this threshold is kept to the lowest level possible, so as to limit the risk that cooperation for analytical purposes can be denied because of lack of information on possible underlying offences: while these latter can in fact vary from country to country, at the stage of analysis of suspicions, where FIUs operate and entertain their cooperation, it may not even be clear if any criminality is involved, not to mention its type.

This issue becomes particularly relevant when a requirement, or an expectation, is in place that, in money laundering-related cases, requesting FIUs should specify the particular predicate offence for which they would be pursuing their analysis and seeking cooperation. Responses show that in some cases cooperation can only be provided when a predicate offence is specified and this is also criminalised, in the same form, in the country of the requested FIU. This condition can unduly pose

[130] See paragraphs 10.2 ff. for a discussion on conditions and modalities, based on the prior consent, for the dissemination or use of the exchanged information for further purposes.

significant restrictions to the FIUs' capacity to cooperate, both because, as said, predicate crimes are difficult for FIUs to identify (as to their very existence and type) at the stage of analysis of suspicious financial activities (which is where international cooperation takes place) and because crimes may well differ under criminal laws of Member States.

On this point, not all FIUs seem to be fully in line with the requirement in the fourth Directive to provide cooperation "even if the type of predicate offences that may be involved is not identified at the time of the exchange" (article 53(1)).

On this point, a respondent emphasized that "information can be exchanged independently of whether a predicate offence is identified. However, where any information is provided as to the underlying criminal conduct, this has to constitute criminal conduct also in [our Country] for [the FIU] to exchange information with the requesting FIU. Whether criminalisation is in the same form or otherwise is not important".

Another respondent underscored that "a link to at least a suspicion of crime / criminality, with some expansion of what that crime or criminality is, has to be there to judge that any dissemination is ECHR compliant, that is justified, proportionate and necessary. Also, if it is not a crime in the country receiving the request, then a dissemination is not justified".

1.4 Police and judicial FIUs: separation between FIU's cooperation and law enforcement or judicial cooperation

Analysis is intrinsically different from law enforcement and prosecution and is subject to a different legal framework. FIUs that have a police or judicial nature and that may be in charge of both need to keep the two functions rigorously separate. On this point, while respondents generally confirm that this separation is ensured in most cases, the Survey highlights areas of potential problems associated with this cross-cutting issue.

Chapter 1 describes how differences in EU FIUs' status and institutional organization can affect the nature and type of the functions performed, differently from the "paradigm" that seems to underlie the EU provisions that allows for flexibility in this regard. The "analysis" function, in lack of a common definition, may take on significantly different forms across Countries and, especially for FIUs that have a police status, may become difficult to discern with respect to investigative activities[131]. Chapter 3 then discusses how the lack of a clear demarcation between analysis and investigation reflects on the EU FIUs' capacity to have access to information, as this can be limited by the absence of a recognised area of autonomous analytical function for the FIUs; as a consequence, these may be inhibited or made subject to conditions in accessing information when investigations or legal proceedings are ongoing or when the information needed is considered to be accessible only through law enforcement measures or powers[132]. Moreover, Chapter 5 focuses again on cases where EU FIUs' analytical functions are not kept separate from law enforcement activities and discusses how this impacts on the effectiveness of these functions in bringing added value to ensuing investigations (due to the "confusion" between different steps) as well as on the dissemination function, as STR/SAR information, rather than being forwarded after analysis, can be used upfront for both analysis and investigations (either by the same FIU or even by different agencies).

[131] See, for example, par. 2.4 in Chapter 1.
[132] As seen, this is typically the case of financial information or information held by obliged entities.

Differentiating between "analysis" and "investigation", the former exercised as an FIU and the latter as a law enforcement body, may prove particularly difficult when the two functions are vested in the same agency. These difficulties may be higher when law enforcement-type FIUs are called on to share STR/SAR information with police organs sitting in the same organisation for parallel development through investigation (before and beyond a proper analytical phase). These two approaches seem both present in EU FIUs that have a law enforcement status: some are in charge of both analysis and investigations; others focus on analysis but are required to share STR information with police units in the same organisation.

In these instances, there may be risks that financial analysis and police investigations, rather than being two consecutive steps, the former reinforcing the latter and bringing added value to it, could overlap and be merged, with financial analysis ending up being absorbed into investigations and deprived of an autonomous role. The FIUs' capacity to act as such and exercise autonomous powers to obtain information and conduct analysis prior to and independently from investigations could also be affected in these cases, with implications on both effective domestic analysis and cooperation with other FIUs.

Inevitably, in fact, cases where the analysis tends to be merged or absorbed into law enforcement activities, either due to the status of the FIU or otherwise to the lack of a clear distinction between different activities, along with consequences at the domestic level on the FIUs' effectiveness and capacity to obtain information and exercise powers, also bring consequences on the FIUs' ability to engage properly in FIU-to-FIU cooperation. The same conditions or limitations that affect the FIUs' functions and powers also apply when it comes to provide cooperation to foreign counterparts. This happens, for example, because FIUs could have a limited capacity to exercise independent powers to gather information needed to foreign counterparts, either because it is prevented from doing this due to ongoing investigations or because it is subject to an authorisation by a competent law enforcement agency or prosecutor; equally, FIUs' may be prevented from providing information to foreign counterparts because, for example, this information can only be shared through police or judicial cooperation channels.

While, as said, the majority of EU FIUs having a law enforcement or judicial status have indicated in their responses that cooperation and exchange of information with other EU FIUs is a separate task from law enforcement and judicial activities and cooperation, the analysis of responses specifically addressing the capacity to provide cooperation (through the initial exchange of information and the ensuing consent for further use or dissemination) reveals that in some cases those same respondents face constraints associated with, for example, the need to use police or MLA channels to obtain certain information and the need for an authorisation in order to be able to share data.

As also said[133], a respondent has indicated that the FIU's cooperation is not separate from law enforcement activities. One practical implication, highlighted by the same respondent, is that requesting FIUs are expected to describe the underlying criminality. This requirement, although it does not go so far as to entail the reference to particular types of crimes, apply to both the exchange phase and to the subsequent request for consent for further use or dissemination of the information exchanged (as recalled above, on the contrary, the Directive foresees that the exchange should take place even if the possible predicate offence is not known).

[133] See Chapter 5, par.2.2.

1.5 Capacity to use domestic powers to obtain and provide information to foreign counterparts

The majority of respondent FIUs have indicated that they are empowered to use the same domestic powers available for their own analysis when it comes to obtaining information needed to provide cooperation to foreign counterparts. While par. 4 will discuss this point in more details, some considerations need to be developed here as regards the general capacity of EU FIUs to provide cooperation by making use of their domestic powers.

In many cases, this capacity is rooted in general domestic provisions enabling the FIU to have access to information sources for discharging its functions, rather than in ad-hoc rules specifically implementing this innovative requirement brought about by the fourth Directive (in line with pre-existing FATF standards). It remains to be seen whether this generic approach to empowering FIUs to use their powers for international cooperation purposes, should it not be complemented with more specific provisions in the forthcoming legislation implementing the Directive, will generate difficulties in the practical application of this essential new feature of FIUs' cooperation.

On this note, respondents are already flagging possible elements for further reflection or consideration. For example, some have indicated that a "proportionality" approach has to be applied to gathering and sharing requested information (depending on, for example, the type and the relevance of the case for whose analysis cooperation is sought), to avoid that an excessively wide range of available powers is activated to address scarcely important cases.

Also, data protection concerns have been flagged arising from a potentially broad access to domestic information for international sharing purposes, without adequate justification.

More in general, a need to determine the extent to which domestic powers have to be used to respond to requests from other FIUs has been mentioned by respondents: should this be based on a case-by-case evaluation done by the requested FIU or all available powers have to be exhausted in each case?

An important consideration in this context is the need for appropriate description and motivation at the basis of requests. Several respondents emphasize that to a broader duty for requested FIUs to provide assistance by means of all available powers should correspond a reinforced obligation for requesting FIUs to submit duly motivated and substantiated requests, particularly as regards the description of the case under analysis, the grounds for the suspicion, the links with the country of the requested FIU, the information sought[134].

While requests certainly have to be properly motivated, this requirement should be weighed against the need to not overburden requesting FIUs, also keeping in mind that the Directive foresees that exchanges can be performed also in the absence of substantiated requests (see on this article 53(1)[135]). Due to an excessively high threshold for requests, FIUs could be inhibited to receive cooperation when, as is typically the case at the initial stage of analysis, the context may not be yet entirely defined. At the same time, it is important to avoid that possible requirements concerning the

[134] See Article 53(1) of the fourth Directive on the requirements for requesting FIUs.

[135] After a first sentence mandating that requests should be motivated ("A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used"), the second sentence allows for "different exchange mechanisms", which can be applied "if so agreed between the FIUs", whereby exchanges may take place without any particular requirement for the request. This provision (which in fact explicitly references the "exchanges through the FIU.net or its successor"), provides the legal basis for "Known/Unknown" interactions: see par. 6.

information content of the requests and the need for proper motivation are used by the requested FIU to perform an autonomous assessment of the case and decide whether or not it deserves a follow up, regardless of, or even in contrast with, the same assessment that had led the requesting FIU to ask for assistance[136].

The obligation to use domestic powers to respond to foreign requests needs to be better rooted in national legislations, particularly through an explicit and dedicated legal basis which unequivocally empowers the FIU to use its powers on behalf of other FIUs.

At the same time, details should be provided on the extent and scope of this duty, to avoid both uncertainties in national implementation and different and differing approaches being taken by requested FIUs. Provisions or guidance in this regard should be set out at the EU level.

For example, clarifications would be helpful on the need to exercise domestic powers with a view to providing the most appropriate assistance possible in light of the case and commensurate to the information needs of the requesting FIU. Also, available powers should be used, and information sources accessed, taking account of concurrent elements such as the specific demands formulated by the foreign counterpart, the features of the case underlying the request, possible elements on the case which are available domestically (as a consequence, for example, of ongoing analyses or investigations or the involvement of particular subjects).

While reiterating the importance of well-motivated requests for this purpose, as they should allow the requested FIU to understand the case and the related information needs of the counterpart, it should be clarified, at the same time, that insufficient motivation cannot be per se a valid ground for declining requests for cooperation and, more specifically, to refuse to exercise domestic powers to obtain information. In such cases (as will also be discussed later in this Report), counterparts should enter into a dialogue to clarify the context of the request, the information needs and target the exchange accordingly.

1.6 Need for memoranda of understanding as a precondition to cooperate

Differently from the FATF and Egmont standards, which allow for the possibility that FIUs' capacity to exchange information to be subject to the prior definition of memoranda of understanding (MoUs), the duty for EU FIUs to cooperate and exchange information is unconditional under the Directive. The sharing of information among EU FIUs, therefore, cannot be made subject to prior MoUs.

Against this background, which was in place already before the current fourth Directive[137], responses to the Survey confirm that EU FIUs have a direct capacity to exchange information, based on their respective domestic laws and with no need for ad hoc prior agreements entered into with counterparts from other EU Countries.

[136] On this, see more in paragraphs 2 and 9.

[137] Cooperation among FIUs was previously regulated by Council Decision 2000/642/JHA, which has not been repealed by the 2015 fourth Directive (the third Directive 2005/60/EC did not deal with FIUs' cooperation). Under the Decision, the duty to exchange information is also an unconditional obligation for FIUs which cannot be made subject to prior agreements; MoUs are recognized by the Decision under article 9 but only "to the extent that the level of cooperation between FIUs as expressed [in such MoUs] is compatible with this Decision or goes further to the provisions thereof".

1.7 Condition of reciprocity

Due to the common legal framework, as set out by the fourth Directive and by domestic implementing legislations, it is expected that provisions applicable to FIUs and to their cooperation are particularly homogeneous across EU Member States, thus making the condition of reciprocity superfluous[138]. At the same time, there is also an expectation that, being the FIU-to-FIU cooperation within the EU particularly close and integrated, as well as consolidated through several years of experience, FIUs do not need to apply "defensive" mechanisms against lack of adequate responses and cooperation from counterparts due to differences in the levels of assistance provided and, therefore, should not be allowed to refuse to exchange because of the lack of reciprocity.

More precisely, because of the highly homogenous ground upon which FIU-to-FIU relations rest within the EU, an assumption may be in place that similar or equivalent conditions apply across different Member States, in terms of EU FIUs' capacity to obtain and share different types of information. As a consequence, "reciprocity" would become intrinsically fulfilled as an embedded element in exchanges among FIUs and, consequently, the reciprocity condition would simply be superfluous.

As a matter of fact, against this background and based on these assumptions, the fourth Directive (in line with pre-existing EU provisions on FIUs' cooperation) does not envisage or, at least, does not explicitly mention, the condition of reciprocity as a prerequisite for EU FIUs' cooperation. As a consequence, it seems that EU FIUs should not refuse or limit cooperation with other EU counterparts on grounds of lack of reciprocity.

However, responses to the survey indicate that, based on domestic laws, the majority of EU FIUs are bound by the condition of reciprocity and apply this condition to counterparts from other Member States. This results in restrictions to the capacity to exchange information and provide cooperation in potential contrast with the provisions of the fourth Directive.

The condition of reciprocity can play adverse effects on international cooperation, both as regards its extent and its effectiveness. These effects can be amplified by the enlargement of FIUs' powers and capacity to access information, as realised by the fourth Directive, and by the continued existence of differences and discrepancies among national frameworks, as also allowed by the Directive, particularly in the absence of sufficiently detailed and uniform indications on types and extent of information and powers that should be available to FIUs.

[138] The condition of reciprocity, in fact, allows FIUs to make the provision of assistance subject to the verification that the requesting counterpart would be able to provide the same assistance had it been requested in a similar case or under similar circumstances. This gives FIUs a defence against counterparts with less information or powers and, and the same time, provides incentives to these counterparts and their countries to expand the capacity to provide cooperation (as this would become a condition to also receive assistance).
"Reciprocity" lends itself to different interpretations as regards its scope. Under a stricter interpretation, cooperation may be refused because of lack of reciprocity in cases of any differences in individual information sources or powers between the counterparts involved ("I can give you exactly what you can give me"). A different and broader understanding of "reciprocity" is also possible, whereby this condition is considered to be fulfilled when, regardless of a precise correspondence between the information exchangeable or powers exercisable, the counterpart provides the assistance it can lend based on its laws and on a "best effort" basis, without declining it in circumstances other than those admissible for the requesting FIU in similar cases or circumstances ("I give you what I can if you give me what you can").
Clearly, the former understanding of reciprocity is more likely to pose significant limitations to FIUs' cooperation, as any difference in information or powers could justify refusals; at the same time, it would create strong incentives to FIUs, and their countries, to expand their capacity to cooperate as this becomes a condition to obtain information when this is needed.

While, under the EU legislation, FIUs should have a broad access to a wide range of information and dispose of extensive capacities and powers, both domestically and internationally, significant differences continue to be allowed (and continue to exist in Member States, as also reflected in this Survey) among national regimes. These differences affect, i.a., the range and types of information available, the scope of the powers exercisable (e.g. for performing enquiries or postpone suspicious transactions), the capacity to cooperate due to existing conditions or limitations.

In all areas where differences exist reciprocity can be lacking, despite the common (but not sufficiently uniform) EU legal framework. Each such area can host a number of potential triggers for the reciprocity condition to apply, thus obstructing FIUs' cooperation. The sharing of information can be prevented or limited depending on the conditions applied by the counterparts involved and the differences between the regimes to which they are subject. The combined effect that discrepancies and reciprocity can have on the capacity of EU FIUs to provide adequate cooperation cannot be underestimated[139].

The following points, also based on elements specifically flagged by respondent FIUs in different sections of the Questionnaire, try to address and highlight areas where the lack of the reciprocity condition seems more likely to arise and its effects appear more prominent.

- Types of information. The range and types of information that should be available to FIUs for their analysis and for international cooperation are not specifically determined by the Directive[140]. Article 32(4) only stipulates that FIUs should have access to "the financial, administrative and law enforcement information that they require to fulfil their tasks properly". No indication is provided as to what specific sources of information qualify, respectively, as "financial", "administrative" and "law enforcement" or on when FIUs' tasks can be considered to be fulfilled properly, based on the range of information available. In the absence of more detailed indications on information sources or databases which should be available to FIUs as a minimum[141], national approaches vary greatly. This is the case, for example, of the "financial" information, whereas several FIUs receive less information than other on banking transactions in STRs/SARs and do not have access to data on bank accounts or financial transactions[142].

  Several respondents have flagged this as a potential obstacle to the exchange of information due to reciprocity: FIUs with a bigger capacity to receive or access financial information are reluctant to share all this information with foreign counterparts with lesser access to data which could not reciprocate if requested under the same circumstances.

  For example, one respondent has clearly indicated that, while it has access to information on bank accounts through a centralized database (or retrieval system), it is not in a position to provide this information to counterpart FIUs that cannot provide the same information due to the lack of such data source in their countries.

- Exercise of domestic powers to obtain information on behalf of counterpart FIUs. The Directive requires FIUs to exercise the same domestic powers available for their analyses in order to provide assistance to other EU FIUs (article 53(2)). Some of these domestic powers

[139] Especially if "reciprocity" is interpreted broadly: see footnote 139.
[140] This point is specifically examined and discussed in Chapter 3.
[141] With the notable exception of the information on beneficial ownership which, under the Directive, should be gathered in central national registers available to FIUs and other competent authorities (see article 30 and 31).
[142] See Chapter 3, par. 5, on the availability of information allowing to identify whether national or legal persons hold accounts with banks within the territory of each Member State.

are referenced in the Directive[143] but these references are neither exhaustive nor regulated in details[144]. In addition, the extent to which the available powers should be exercised to respond to foreign requests is also not specified in the Directive. This results in significant differences among EU FIUs, as regards both the range of available powers (namely, for accessing information or query third parties) and the extent to which these powers can be activated on behalf of foreign counterparts.

Respondents have highlighted that reciprocity considerations are particularly important in this area, as many of them would not exercise powers to assist counterparts that do not dispose of the same powers or would not use them for international cooperation purposes. Responses also refer to a "proportionality" test, whereby requests are evaluated on a case-by-case basis to determine the extent to which domestic powers should be mobilized for gathering (from internal or external sources) and providing information to foreign counterparts.

- Capacity to share information with other FIUs. Not only FIUs differ in the types of information available and in the capacity to deploy domestic powers to provide cooperation; they also have different capacities to exchange information with foreign counterparts. If also other conditions had been equal as regards the information available or obtainable (but they are not), FIUs would still remain diverse in their ability to share such information. Respondents report, in fact, that the exchange is often subject to limitations and conditions. These are connected, for example, with the need to obtain prior authorizations from other domestic agencies "owning" relevant information, to the existence of investigations or legal proceedings, to the identification and nature of possible predicate offences, to restrictions concerning tax matters (see Par. …). These conditions, diverse as they are across Member States, limit international cooperation both when they are applied by the FIUs which are bound by them and when they are applied by counterparts which, although not bound by them, apply them nonetheless as a consequence of the condition of reciprocity to which they are subject.

- Capacity to provide the consent for further use or dissemination of the information exchanged. Conditions for providing the prior consent, following the initial exchange of information, also vary from country to country (see par. …). The Directive only establishes that this consent should be given "to the largest extent possible" and identifies general instances where, only, it can be refused[145]; there are no specific indications on particular cases or relevant conditions. Existing differences in FIUs' capacity to consent to further use or dissemination also has a potentially considerable impact on the quality and effectiveness of FIUs' cooperation, both directly and due to "retaliations" triggered by the lack of reciprocity: as also flagged by responses, FIUs that have a broader capacity to provide the consent can be compelled to refuse it when asked by foreign counterparts which would refuse the consent if asked under similar circumstances (despite their legal ability to grant it, had the reciprocity condition been fulfilled). Or, more broadly (as the daily practice of FIUs' cooperation also frequently shows), consent can sometimes only be granted when the

[143] See, for example, Article 32(3) on the FIUs' power to obtain information from obliged entities or articles 30 and 31 on the FIUs' access to national registers with information on beneficial ownership.

[144] For example, the power to obtain information from obliged entities is implemented differently and have a different scope across Member States. On this, see Chapter 4.

[145] Article 55(2) refers to cases where "this would fall beyond the scope of application of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State of the requested FIU, or would otherwise not be in accordance with fundamental principles of national law of that Member State".

counterpart also gives it for the information exchanged on the same particular case at stake. All this goes to the detriment of the possibility to use exchanged information for law enforcement or judicial action against money laundering or terrorist financing, thus significantly affecting the overall effectiveness of FIU-to-FIU cooperation.

- Capacity to provide cooperation to foreign counterparts that are not FIUs. In the absence of provisions in the Directive requiring FIUs to provide information to foreign non-counterparts ("diagonal cooperation"[146]), the lack of capacity to proceed in this respect by an FIU may lead its counterpart FIUs to reciprocate due to reciprocity constraints, thus refraining from sharing potentially valuable information with relevant authorities in the interested Member States (despite their legal capacity to do so in cases where reciprocity is ensured). Also differences in the channels used for diagonal exchanges, when these are allowed by national laws, can trigger undesired consequences via the reciprocity condition: in fact, FIUs that do not use indirect FIU-to-FIU communications to reach out to authorities in other Member States may lead the FIUs in such Member States to equally avoid appraising their counterpart FIUs of sensible STR/SAR information by forwarding directly such information to the final foreign recipient authorities (diagonal cooperation will be specifically discussed in Chapter 8).

- Capacity to share information on cross-border STRs/SARs[147]. Similarly to other potential problem areas where the reciprocity condition can adversely affect FIUs' cooperation, the lack of a common definition or criteria to identify suspicious transactions "that concern another Member State", as well as the possibility to condition the sharing of such disclosures to particular triggers or thresholds (such as the assessed relevance of the case, the absence of legal proceedings, the disconnection from tax matters, etc.) may leave room to different approaches across Member States on the FIUs' capacity to share cross border cases. This can affect the amount and quality of the information shared as a consequence of "cutting off" effects determined by the lack of reciprocity in all cases where different conditions apply to the FIUs involved. Put it simply, FIUs may refrain from forwarding cross-border STRs/SARs, against the provision in article 53(1), to FIUs that do not provide the same information or provide such information under stricter conditions.

- Capacity to engage in joint analyses[148]. Moreover, as joint analysis activities build on information sharing mechanisms which help setting a common ground upon which shared intelligence and outputs can be developed by FIUs, the potential impacts on such information sharing mechanisms from the (lack of) reciprocity as described in previous points is susceptible to make joint analyses more difficult to put in place or not fully effective. These difficulties would add on to, and be amplified by, those which in several cases affect FIUs' capacity to engage in joint analyses, as will be specifically discussed in par. 8.

- Confidentiality and data protection conditions. Differences in the ways in which exchanged information is protected and processed are also a potential source of detrimental effects caused by the application of the reciprocity condition.

One respondent has specifically indicated that its capacity to exchange information is subject, by law, to reciprocity in the confidentiality safeguards applied by foreign

[146] See Chapter 7 for a dedicated analysis on diagonal cooperation.
[147] See article 53(1) of the fourth Directive and par. 5 in this Chapter.
[148] See article 51 of the fourth Directive and Chapter 8 in this Report.

counterparts. Other examples may include differences in data retention periods applied by FIUs: those FIUs bound by shorter retention periods may not be allowed to provide information which would be kept for a longer time by the recipient FIU. Also different types of use of the information exchanged by the receiving FIU (only for intelligence purposes or also for investigations) could raise data protection concerns, with potential further repercussions via the reciprocity condition. Responses show that data protection limitations lie also at the basis of restrictions which prevent some FIUs from accessing and sharing bank account information outside of formal mutual legal assistance exchanges.

In general, moreover, it can be observed that a broad and formalistic interpretation of the reciprocity rule, whereby an FIU bound by it would not cooperate by providing information if exactly the same information or power is not provided or cannot be exercised by the counterpart in the same exchange, or cannot be provided or exercised if requested in similar circumstances (see the considerations in footnote …), can lead to potentially significant effects on FIU-to-FIU cooperation in the EU, against the provision in the fourth Directive. While Member States and FIUs should drop the reciprocity condition entirely insofar as intra-EU cooperation is concerned, it is hoped that they do not apply this condition in a rigid and formalistic fashion on a case-by-case basis[149] but contextualize it having regard to longer-term relations between FIUs and overall trends of cooperation.

While the fourth Directive allows for refusing to exchange information when this contrasts with "fundamental principles" of national law (article 53(3)), it is not clear whether this scope includes the condition of reciprocity (which does not seem to qualify per se as a "fundamental principle"). The reciprocity condition is not recalled in the Directive as a requirement to be fulfilled for FIUs to be able to provide cooperation and, therefore, refusals to provide cooperation on the grounds of possible lack of reciprocity do not seem admissible as they would contrast with the general obligation to provide cooperation in accordance with article 53(1). Clarifications on this point through EU provisions would certainly be helpful. This, in particular, is needed as, in the current framework, several EU FIUs are bound by the reciprocity condition under their domestic laws (as indicated by respondents).

At the same time, work needs to be done at the EU level in support of the assumptions which lie at the basis of the need to provide cooperation regardless of reciprocity considerations, notably that reciprocity among FIUs is embedded in the system due to the high level of harmonization of applicable national regimes, particularly as regards the information available and exchangeable and the powers that can be exercised by FIUs to obtain it.

In fact, a prohibition to refuse cooperation on reciprocity grounds can be maintained only if EU FIUs' become capable, based on a truly harmonized legal framework at EU level, to exchange information and provide cooperation based on equal conditions and on a comparable extent and quality level, thus being able to "reciprocate" any response.

To achieve this objective, a higher level of harmonization seems to be needed, particularly as regards the types of information that should be available to FIUs, the powers (as regards their extent and possible conditions) which should be exercised to obtain information, the capacity to exchange information with other FIUs (as regards conditions or limitations), the ability to provide

[149] That is in a form along the lines of "I can only give you exactly the same information you would give me had I filed the same request to you"; or, as far as the consent for further use or dissemination is concerned, "I only give you the consent to forward the information exchanged if you similarly allow me to forward the information on the same case contained in your request".

the consent for further use or dissemination of the information exchanged.

The areas highlighted above in this paragraph, specifically flagged in the survey, can be considered as priority issues to tackle in this perspective. They are also further described and discussed in other sections of this Report.

1.8 Need for a clearance or authorization from a third party

The vast majority of FIUs have confirmed that they can exchange information freely, with no need for a third party's authorization under any circumstance and for any type of information, either available through STRs/SARs or obtained from external sources. For some respondents, however, the sharing of information is dependent upon authorizations or other forms of clearance issued on a case-by-case basis. For example, some respondents have indicated that when investigations are underway on the same case, an authorization from the competent judge or prosecutor is a necessary condition for the exchange.

A respondent clarified that a permission by the competent prosecutor is required, either for the sharing of information or for the consent to their further use or dissemination, when the following conditions occur: a) a pre-trial procedure has been initiated with regard to the same facts to which the request also relates; b) the information on the case available to the FIU is included in the investigation material; c) sharing this information (or consenting to its further use or dissemination) could negatively affect the ongoing pre-trial procedure.

In the instances where the authorization is not provided and the capacity to exchange information is therefore restrained, due to ongoing investigations or prosecutions, a respondent has indicated that it shares the details of the investigating magistrate (subject to his/her consent) and the procedure to follow, so that the foreign counterpart FIU can facilitate the possible activation by domestic competent authorities of the necessary police or judicial channels for international cooperation.

It is important to underscore that, under the EU legislation, the FIUs' capacity to provide information cannot be limited due to the mere existence of an investigation or a legal proceeding on the same case; the exchange of information can only be denied, "in exceptional circumstances" (thus not systematically), only when it is "contrary to fundamental principles of national law"[150].

When it comes to requests for consent for further use or dissemination of the information provided, the prior consent also cannot be denied due to the mere existence of an investigation or a legal proceeding. A refusal is only justified when, i.a., the dissemination "could lead to impairment of a criminal investigation"[151].

Therefore, under the fourth Directive the general rule of "free exchange of information" among FIUs cannot be derogated in case of ongoing investigations, except under very specific circumstances. It has also to be recalled that situations where the FIU is subject to third parties' authorizations as a condition to provide cooperation do not appear in compliance with the requirements of operational independence, as discussed in Chapter 2[152].

[150] Article 53(3). Even in such exceptional cases, "those exceptions shall be specified in a way which prevents misuse of, and undue limitations on, the free exchange of information for analytical purposes".
[151] Article 55(2). See par. 10 on existing limitations to the FIUs' capacity to provide the prior consent.
[152] See specifically par. 2.6.2 of Chapter 2. Article 32(3) of the Directive clarifies that the independence status entails that FIUs should be able to "take autonomous decisions".

Other respondents highlight that, in order for the FIU to be able to forward to a foreign counterpart information obtained from other domestic authorities (for example, fiscal or custom agencies), a prior permission must be obtained from these authorities.

These also appear to be circumstances where the FIUs' capacity to exchange information freely is unduly restricted. As, under the fourth Directive, FIUs are required to exchange both information already available (typically, that in STRs/SARs or in other disclosures) and information obtained through the exercise of domestic powers, the latter cannot be conditioned to a permission without limiting the overall FIUs' capacity to (freely) provide information.

Yet other responses make reference to "internal authorizations" as a condition to the exchange, either from inside the FIU or from collateral units within the same organization where the FIU is located. As regards authorizations issued by internal staff, these can be considered as part of the ordinary decision-making process within the FIU. They could only raise concerns in cases where the refusal of such internal authorizations would translate in undue refusal by the FIU to provide cooperation, in contrast with EU provisions (that is, outside the narrow exceptions allowed by the Directive).

On the other hand, forms of authorizations given by other units, outside of the FIU although belonging to same bigger organization (for example, in case of potential interferences with ongoing investigations or intelligence activities), may well amount to limitations to the FIU's capacity to freely exchange information, unless, again, these are restricted to cases of refusals allowed under the EU legislation.

The FIUs' capacity to freely exchange information appears unduly limited by cases where the exchange is subject to authorizations or clearance that must be obtained from domestic third parties. This happens especially when investigations or legal proceedings are underway in the country of the requested FIU or where the requested information has to be obtained from another agency. Similar limitations to FIUs' cooperation apply in relation to the release of the prior consent for further use or dissemination of the information exchanged.

While it is important to recall that the process for the implementation of the fourth Directive is not yet complete (although the correspondent FATF standards are in place since 2012), these restrictions seem to depend mostly on the following factors:

- an excessively narrow implementation of the principle of "free exchange of information for analytical purposes" among FIUs (article 53(3) of the Directive, which certainly forbids refusals related to the mere existence of investigations or legal proceedings) and of the duty to provide the prior consent "to the largest extent possible" (article 55(2));
- an excessively broad transposition of the derogations clauses for the exchange and for the prior consent, respectively in article 53(3) (which refers to "exceptional circumstances where the exchange could be contrary to fundamental principles of national law") and in article 55(2).

A more adequate and uniform implementation of these fundamental provisions across EU Member States could be encouraged and facilitated through guidance issued at the EU level, based on legislation or other suitable means, clarifying that the duties to provide cooperation, either through the initial exchange or through the consent for further use or dissemination of the information exchanged, have a general scope and cannot be limited due to the mere existence of investigations or legal proceedings (unless, as far as the further use or dissemination are concerned, these may

impair such investigations or proceedings, in accordance with article 55(2) of the Directive: see more on this in par. 10, esp. 10.4 and 10.5 and the conclusions and proposals in par. 10.9).

1.9 Timeframe for responses. The issue of "timeliness"

All EU FIUs have indicated that they are able to provide timely responses to requests for information submitted by their counterparts. In many cases, a feedback can be given within a week, even less for urgent requests. Several FIUs can react to priorities even in a matter of hours (this may prove particularly important, for example, in cases where funds are being temporarily restrained, e.g. through a postponement order issued by the FIU that requests the information). Many respondents are able to send information in timeframes ranging from two weeks up to two months or more.

Based on the information provided in their responses to the Survey, EU FIUs appear therefore aligned with international standards concerning the timeframes for responses to requests from foreign counterparts[153].

This evidence seems to contrast, at least partly, with the feedback provided by respondents under the last section of the Survey, dedicated to prominent problems or obstacles encountered in the cooperation with other EU FIUs. In that context, in fact, responses have flagged that the timeliness of feedback is a critical area for cooperation and have stressed that current delays in receiving information or the consent for its further use or dissemination from counterpart FIUs may have an impact on the effectiveness of analytical activities and ensuing law enforcement actions[154]. While the indications provided by respondents in the last part of the Survey are certainly useful as a "back test", there is certainly an inconsistency in responses on the same point which makes it difficult to determine whether EU FIUs are in effect providing timely cooperation to their counterparts.

This inconsistency may be explained by the bias deriving from the different viewpoints that respondent FIUs may have taken approaching different sections of the Survey. In reporting about the timeframe of the responses to foreign requests, FIUs have acted as "respondents" or suppliers of cooperation, thus possibly projecting a relatively more optimistic view on their individual capacity to provide cooperation in accordance with appropriate standards, particularly as regards timeliness requirements[155]. On the other hand, in highlighting the problems they commonly encounter in obtaining cooperation (in the last part of the Survey), FIUs have responded from the "demand" side, that is as requestors of cooperation; for this reason, they may have taken a more rigorous or negative approach, rather inclined to emphasize the delays in others' responses.

Whatever the reason may be for this inconsistency, the discussion on the timeliness of FIUs' cooperation remains inconclusive, particularly due to the lack of more objective information or data on which any assessment should be based.

A solution to this possible bias, and to the associated difficulty in understanding the current status of FIU-to-FIU cooperation in the EU as regards the capacity to respond timely, can be found in the setting up of a rigorous system of comprehensive statistics, common to all EU Member States, allowing to compare data and gauge the performance of, in this case, FIUs in their reciprocal

[153] The "Operational Guidance for FIUs' Activities and the Exchange of Information" of the Egmont Group stipulate that FIUs should be able to respond within one month, if possible, whereas "additional time is reasonable if there is need to query external databases or third parties" (n. 21).
[154] See Chapter 9, par. 13.
[155] It is important to underscore that responses on this point are based on a self-assessment by FIUs and do not carry ad-hoc data in support of the indications provided.

cooperation. Information about timeframes and delays in providing different forms of cooperation, taking account of types of requests and also of the complexity of the cases and of the need to exercise different information powers for gathering the necessary data, should be consistently collected and made available by Member States and FIUs, in formats that allow cross-comparability.

This would permit, for example, to compare statistics gathered from FIUs in both their "requesting" and "responding" functions, thus identifying and solving possible discrepancies or inconsistencies between the demand and the supply side, as regards the timeframes, and come to a coherent assessment on the effectiveness.

This objective may be achieved, for example, through appropriate implementation of article 44 of the Directive, which required Member States "to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics", including "data regarding the number of cross-border requests for information that were made, received, refused and partially or fully answered by the FIU". It is important to bear in mind that, in a EU-wide perspective, there is a need for cross-comparability and uniformity of data collected, which calls for a harmonized approach to how statistics are build and data gathered, especially on matters that have a cross-border dimension, such as FIU-to-FIU cooperation. For this purpose, a common system of data gathering should be defined at the EU level.

1.9.1 Timeframe for responses. Factors that affect timeliness

Respondents have indicated that shorter reaction times are normally possible for providing feedback based on information already available to the requested FIU. On the contrary, the response time increases when the information has to be obtained from external sources, namely by approaching or asking other authorities or by obtaining data from obliged entities. In these cases, respondents have reported that it is difficult to estimate average response times.

Another factor that respondents have highlighted as considerably influencing the timeframe for responses is the significant, and increasing, volume of exchanges and incoming requests. This, coupled with resource constraints, leads FIUs to adopt an approach based on the accurate selection of priorities, in light of the level of urgency flagged by the requesting counterpart and the nature of the case.

On the other hand, the use of advanced IT tools for international exchanges (notably, the FIU.NET), often integrated in FIUs' internal systems for accessing and sharing information, allows for considerable efficiency gains through easier and speedier processing of the requests through data matching and retrieval.

Several FIUs have reported, in response to the Survey, sufficiently detailed data on their timeframes for providing cooperation to foreign counterparts. However, such data does not seem always based on accurate and systematic statistics (see also considerations in the previous paragraph). While keeping statistics in this area may not be easy (especially due to the need to retain information, which is neither uniform nor standardized, on variable response times to domestic inquiries for obtaining the information needed for the international exchanges), they certainly are an essential tool for measuring and improving the FIUs' performance and maintaining efficiency through appropriate internal review.

Interestingly, a respondent has reported that it has internal controls and management systems in place whereby all FIU's operational activities, including international cooperation and its

timeframes, are reviewed on a weekly basis.

Internal controls and reviews on operational activities are certainly useful tools to make sure that the FIU maintains adequate procedures, using its resources consistently with the workload and the priorities, as they evolve over time, also as far as international cooperation is concerned.

The increasing volumes of domestic disclosures and foreign requests add on to the FIUs' workload and put considerable pressure on available resources. In this context, it is important that the need to provide adequate and timely cooperation to foreign counterparts continues to be considered a priority by EU FIUs. To emphasize this aspect, and reinforce the duty to provide responses in a timely manner, the obligation set out in this respect under article 53(2) could be further specified to provide for more details and specific timeframes (in line, for example, with the standards of the Egmont Group) to take account of factors such as:

- the nature of the case underlying the request and the level of priority indicated by the requesting FIU;
- the information needs associated with the request and the underlying case;
- the availability of the information requested or the need to obtain it from external sources or third parties.

The use of advanced IT tools to retrieve data (see article 56 of the Directive), the collection of dedicated statistics on international exchanges in their various forms and the implementation of internal controls and review in this matter are also elements that could be taken up by EU legislation or guidance to foster FIUs' timely and effective cooperation.

2. Cases where the exchange of information can be refused

The capacity to provide cooperation through the exchange of information, a fundamental and essentially unconditioned function for FIUs under the fourth Directive, seems to be well established across Member States. Nonetheless, there are significant exceptions that appear to exceed the scope of the derogations allowed by the EU legislation (and by international standards as well). The Directive allows for refusals to the exchange only under very limited circumstances (see article 53(3)). These can only be rooted in "fundamental principles" of national law which may be exposed to violation; in addition, the exceptions should be specified ex ante (in national law or regulation), in a way which prevents misuse and does not unduly limit the general rule of "free exchange of information for analytical purposes". Therefore, refusals to exchange should be limited to exceptional cases, to be specified domestically, and the general obligation to share information (all relevant types, either available or obtainable through queries or domestic powers) should be applied unless national fundamental principles may be at stake.

It is important to recall that cases of refusal of the consent for further use or dissemination of the information already exchanged are dealt with separately in the Directive, which allows for a broader scope for such refusals under article 55(2). It is also important to recall that refusals to exchange information can consist in outright denials to provide a feedback to requests from other FIUs in certain cases or under certain conditions but can also derive from prohibitions to share particular types of information, unless some conditions are met or particular circumstances occur. This paragraph deals with cases where FIUs are allowed or obliged, under their domestic laws, not to engage in exchanges of information with foreign counterparts at all; instances where cooperation is only partially refused, due to the lack of capacity to share particular types of information or the

existence of constraints or conditions to this exchange, will be discussed in the following paragraph (about the completeness of the information exchanged).

Clearly, requests to share information can also be declined not because the requested FIU lacks the capacity to engage with its counterparts but simply because it does neither possess the requested information nor can obtain it by means of its powers. These instances of lack of cooperation due to lack of available or obtainable information are probably the most widespread and frequent in practice and perhaps also the most difficult to address. Problems here lie not in the FIU's capacity (or willingness, for that matters) to cooperate with counterparts from other countries but rather from a limited domestic capacity to have access to information.

A survey of these shortcomings, therefore, should go beyond the consideration of the general FIUs' capacity to engage in cooperation and should also be based on an evaluation of how broad the range of available information is for FIUs in their domestic context. The overall capacity of FIUs to provide cooperation (which evidently goes hand in hand with the capacity to perform properly its analytical tasks, the two being both a function of the adequacy of the information available), therefore, should be judged under these two complementary perspectives: the extent of their access to information at the domestic level and the capability to share information freely with other FIUs.

The link between these dimensions of FIUs' prerogatives is made explicit in the Directive, at least, in two circumstances. On the one hand, under article 32(4), which states that FIUs should have access to the relevant information ("financial, administrative and law enforcement") "that they require to fulfil their tasks properly": reference to "tasks" encompasses both domestic functions (especially analysis and dissemination) and the duties of international cooperation. On the other hand, article 53(2) establishes that, when an FIU receives a request for information from a foreign counterpart, it "is required to use the whole range of its available powers which it would normally use domestically for receiving and analyzing information". Based on this principle of "equivalence" between domestic powers to access information and the capacity to provide cooperation to other FIUs, this latter becomes strictly dependent on the former.

It is therefore particularly important that FIUs are empowered under domestic law to access a broad range of information. This aspect, discussed separately in Chapter 3, has to be considered, as said, as an integral part of the analysis of FIUs' capacity to exchange information through cooperation with foreign counterparts.

Unfortunately, the fourth Directive, while introducing more detailed provisions on the need for FIUs to share information with their counterparts, does not add much in terms of defining a minimum range of information which must be made available or accessible to FIUs domestically[156]. Article 32(4) is only stating that FIUs should have access to, generically, "the financial, administrative and law enforcement information that they require". Based on this tautological provision (carried forward from the previous third Directive), Member States are left with ample discretion. As a consequence, the extent, range and types of information available to FIUs vary widely across the EU, with tangible impacts on both domestic activities and the capacity to provide FIU-to-FIU cooperation under adequate standards[157].

[156] An important innovation in this area though has been the obligation for Member States to empower the FIUs to obtain information from obliged entities: see article 33(1)(b) and Chapter 4.

[157] The issues surrounding the range and diversity of the information available to, ar accessible by, EU FIUs have been recalled and discussed in Chapter 3. See also the considerations and proposals on these aspects in par. 1.7, as regards the implications of this diversity for the reciprocity condition. Further considerations on these aspects will be developed in par. 3.

2.1 Cases for refusal to cooperate

As regards the capacity to engage in the exchange of information "per se" (that is, regardless of the extent and types of the information that can be exchanged), on a positive note all EU FIUs have indicated that this is not conditioned by the existence of prior STRs/SARs: cooperation can be provided, by sharing information, also when the requests concern cases that have not been previously reported to the requested FIU. Unfortunately, despite this positive feedback, as also discussed in this Report, in some cases the existence of prior STRs/SARs becomes relevant as a condition to obtain or provide certain types of information in response to foreign requests. This is the case, for example, of information that has to be obtained from obliged entities, as discussed in Chapter 4.

2.2 Existence of investigations or legal proceedings

On the contrary, there are cases where the exchange is refused due to the mere existence of investigations or legal proceedings in the country of the requested FIU. Importantly, these cases are different from those previously discussed in this Chapter (par. 1.8). These latter concern situations where, due to the existence of investigations or legal proceedings, the FIU needs an authorization from the competent prosecutor or judge as a condition to be able to share information with a foreign counterpart (which thus remain possible). Differently, the cases considered here consist in outright prohibitions for the FIU to share information, regardless of the circumstances or of possible authorizations, because of the mere existence of investigations or legal proceedings.

A respondent has clarified that requests for information have to be refused due to the existence of a criminal investigation underway and the consideration that disclosing the information could hamper this investigation. The response also refers to plans to review these constraints to bring the national legal framework in line with the fourth Directive.

It appears that, either because of the need to obtain ad-hoc authorizations on a case-by-case basis or due to outright prohibitions to exchange, FIU-to-FIU cooperation is still significantly affected by the existence, in the country of the requested FIU, of investigations or legal proceedings, in contrast with the rule of "free exchange of information for analytical purposes". These constraints and limitations may become even more significant, after the initial phase of the exchange, when it comes to providing the consent for further use or dissemination of the information transmitted (see par. 10, esp. 10.4, in this Chapter).

A better implementation by Member States of EU rules on these aspects is certainly needed; at the same time, existing EU rules could be clarified and strengthened, particularly by narrowing down the scope for derogations to the FIUs' duties to cooperate, even in presence of investigations or legal proceedings. The considerations elaborated on these deficiencies in par. 10 and the proposals to address them by allowing to forward the exchanged information to law enforcement or judicial bodies for possible MLA initiatives should also be recalled here.

2.3 Identification and type of predicate offences

Other significant constraints and limitations to the FIUs' capacity to exchange information derive from requirements concerning the indication in the request of the underlying predicate offence and to the type of this offence. Precisely because FIUs perform analysis (that is, they do not gather evidence) on suspicions (that is, facts that may not reveal well delineated features of particular crimes), the exchange of information for this purpose, differently from what happens in the context

of police or judicial cooperation, cannot depend on the identification of particular offences or be conditioned to the type or nature of these offences.

Obviously, in order to trigger FIU-to-FIU cooperation it is still necessary that the analysis pertains to suspicions of potential money laundering or terrorist financing. To satisfy this condition, FIUs are required to substantiate their requests by providing appropriate background information, as foreseen by article 53(1) (see par. 9). Understandably, however, the need for motivation does not entail that particular predicate offences must be identified (see again article 53(1), which will be discussed immediately below).

Under the fourth Directive, the exchange of information among FIUs cannot in principle be conditioned to the indication of a particular predicate offence or to the nature thereof. However, the provisions on this matter retain a certain level of vagueness. As regards the initial exchange, article 53(1) stipulates that information must be shared "even if the type of predicate offences that may be involved is not identified at the time of the exchange". This provision seems to entail that at a later stage of the analysis a predicate offence may well be identified by the FIU and that this may become relevant as a condition to provide cooperation, notably through the consent for further use or dissemination of the information transmitted.

In addition, article 57 of the Directive states that "differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU, to the greatest extent possible under their national law". This provision conveys the idea, first of all, that crimes (at least tax crimes, as they are specifically mentioned) can or should be identified and specified in FIU-to-FIU cooperation[158] and, secondly, that on this basis differences between national criminal laws may justify refusals to provide cooperation (both the initial exchange for analytical purposes and the ensuing consent for further use or dissemination), as this is due in such cases not unconditionally but only "to the greatest extent possible".

Also due to the considerable differences among criminal laws in Member States, this provision represents a significant derogation to the general principle of "free exchange of information" among FIUs as well as to the duty to grant the prior consent "to the largest extent possible" (articles 53(3) and 55(2)).

Although responses seem to indicate that only few FIUs have a necessity to receive, in the requests filed by foreign counterparts, an explicit reference to a predicate offence of money laundering and a description of such predicate offence, some respondents highlight that the exchange of information can indeed be refused when a possible predicate offence related to the case for which cooperation is sought is not criminalised (or not criminalised in the same form) in the country of the requested FIU.

Some FIUs in this group have also clarified that, in order to be able to provide information, the request should outline a case of potential money laundering (or terrorist financing), a link with a suspected predicate crime and its nature, so that the proportionality of the requested assistance can be evaluated (the type and seriousness of the suspected offence is taken into account for this purpose).

Although these limitations to the exchange of information among FIUs for analytical purposes have the potential to impact significantly the scope and effectiveness of FIUs' cooperation and activities,

[158] Differently, in fact, there would be no need for a provision dealing with cases of differences between national criminal laws in the context of FIU-to-FIU cooperation.

there is a shared perception (and an associated expectation) that they are scarcely applied in practice. As a matter of fact, based on responses to this section of the Survey[159], what seems to matter most for EU FIUs that face these constraints is that requests are duly motivated, clearly showing that the underlying case is indeed a potential money laundering or terrorist financing case. Sufficient references to the possible predicate crimes should be included for this purpose.

Nonetheless, having in mind that these shortcomings become more prominent at the "prior consent" phase, when further use or dissemination may be requested (see par. 10, especially par. 10.3, in this Chapter), they should be removed or clarified, also through a more precise and rigorous common legal framework at the EU level.

On this note, it is also important to emphasize that, perhaps not surprisingly, responses indicate that cases where cooperation is refused because of differences in the criminalisation of predicate offences often concerns tax matters. In some instances, this constraint is limited to tax evasion; in others, cooperation seem still possible if it is demonstrated that the analysis for which the cooperation is sought is not on the predicate fiscal crime but rather on the ensuing associated money laundering.

FIUs' cooperation, carried out to support the essential analytical function, should not be conditioned by the consideration of possible predicate offences underlying the case subject to analysis. Neither the existence of a particular offence nor its type or nature should become an element of consideration for the requested FIU to provide cooperation. More specifically, this cooperation should not be refused due to the lack of indications about particular offences, their nature, or the existence of corresponding offences in the domestic legal framework.

This is true both as regards the initial exchange and the subsequent consent for further use or dissemination of the information exchanged, although in this latter case the consideration of existing investigations or legal proceedings and of their object may play a role (see on this the analysis and comments in par. 10).

While Member States should ensure an appropriate implementation of existing provisions in the fourth Directive which prevents FIUs from refusing cooperation due to considerations on the underlying offences to a certain extent, these EU provisions should be clarified and strengthened to better reflect the general rule of cooperation and free exchange of information among EU FIUs. More specifically, current provisions in articles 53(1) and 57, as recalled, retain references to predicate offences that may imply that FIUs could or should, at least in some cases, indicate particular types of crimes in their request and that these indications could influence the extent of the cooperation that should be lent. These provisions should be clarified by more clearly stating that FIUs' cooperation, particularly at the stage of the initial exchange for internal analytical purposes, should not be conditioned to the indication of particular offences or to the type of such offences.

[159] See, however, the feedback provided by FIUs to the last section of the Survey, where, as discussed in Chapter 9, problems related to the indication of underlying predicate offences and their nature are recalled as an obstacle to FIU-to-FIU cooperation. Similarly to what has been recalled above in relation to the issue of timeliness of responses, it is important to bear in mind that FIUs may have provided responses under the different perspectives of providers of providers and of receivers of cooperation: in the fomer case (which is relevant to this Chapter), the importance of indications concerning the underlying predicate offences may have been underestimated, whereas this issue has been flagged as more prominent as an obstacle to receiving information.

2.4 Motivated requests

As indicated, requests for cooperation should be properly substantiated. The case under analysis needs to be described and the grounds for suspicion fully outlined, together with the links identified with the jurisdiction of the requested FIU, thus allowing this latter to understand the information needs and provide the necessary cooperation. While these requirements are recalled in article 53(1) of the fourth Directive as obligations for the requesting FIU, they are also relevant for determining the cooperation duties of the requested FIU (for example, as regards the information to gather and the powers to exercise to satisfy the needs of the requesting FIU).

Responses to the Survey show that for several FIUs the adequate description of the case represents an essential prerequisite for being able to share information: this can only be provided when the case under analysis is adequately described in the request and the underlying money laundering or terrorist financing suspicions are properly indicated.

While the majority of EU FIUs require motivated requests as a condition to respond, only some of them would simply refuse cooperation when this condition is not fulfilled. In several cases, in fact, rather than a straightforward rejection in case of poorly motivated requests, the requested FIU can provide a partial response, due to the lack of sufficient ground and motivation for accessing available domestic sources.

For example, some respondents have indicated that, in the absence of adequate motivation, they can only access certain information and cannot inquire external sources or other domestic agencies. Responses can still be provided, at least to the same extent applicable to "known/unknown" exchanges that, by definition, lack motivation and only aim at detecting "matches" (and are referred to in the fourth Directive in article 53(1)). In addition, partial responses to unmotivated requests can be accompanied by an invitation to provide a more complete background, so that the requested FIU can conduct further searches and share more detailed information.

Besides the mere description of the case, particular importance is attached to the understanding of the grounds for suspicion. For several respondents, this has to be properly explained, clearly indicating that the case is about potential money laundering or terrorist financing. Based on the information provided in the responses to the Survey, it appears that FIUs, while in many cases they specifically require that the grounds for suspicion be adequately detailed, rely normally on the description and evaluation made by the requesting counterpart. The suspicion detected by the requesting FIU, as described in the request (and, if needed, further substantiated through appropriate follow-up exchanges), is therefore recognised as a valid ground by the requested FIU for gathering and sharing the information needed, also through the exercise of domestic powers, under the same conditions applicable in cases of "own" suspicion.

As regards other conditions that EU FIUs need to see fulfilled in requests in order to be able to share information, these concern mostly the reference to links with their countries and the complete and correct identification of persons and companies involved, allowing the necessary searches to be performed with accuracy.

It is indeed important that FIUs, when requested for cooperation and provided with appropriate motivation in accordance with article 53(1) of the Directive, do not refuse to share the information because they assess the case, and the inherent suspicion, differently. Second-guessing the suspicious nature of a case underlying a request and refusing cooperation on this ground would go against FIUs' obligations to cooperate.

In this regard, however, a respondent has indicated that in certain circumstances the existence of suspicions of money laundering or terrorist financing can be challenged.

On this point, it is important to recall that the fourth Directive, while setting out the two "twin" obligations to provide cooperation (article 53(1), for the requested FIU) and to file properly motivated requests (article 53(1), second paragraph, for the requesting FIU), does not make it explicitly clear what is the relation between the two and, more particularly, whether the duty to cooperate may not apply in relation to requests that are not adequately motivated.

To avoid undesired effects on FIUs' cooperation, or uneven applications of these provisions by different FIUs or Member States, the following clarifications, if reflected in EU provisions or guidance, would be particularly beneficial in support of appropriate national implementation and uniform FIUs' practices.

- The rationale behind the obligation to file motivated requests is not to allow the requested FIUs to assess the case by second-guessing it and decide whether and to what extent cooperation should be granted; it is rather about allowing the requested FIU to understand the case and the information needs in order to provide the counterpart with appropriate cooperation.
- In fact, the general obligation to provide cooperation in support of the analysis of potential money laundering or terrorist financing cases, as stated in article (53(1), has an absolute nature and cannot be derogated for the simple reason that requests do not bring adequate information.
- In case of poorly motivated requests, therefore, the cooperation should not be refused; while the requested FIU should provide any possible initial feedback (for example, based on available STR/SAR information), the involved FIUs should enter into a dialogue to clarify the case and the information needs.

2.5 Other factors

In full conformity with the fourth Directive, which establishes that FIUs should cooperate with each other "regardless of their organisational status", all respondents have indicated that they can exchange information with FIUs that have a different nature (administrative, law enforcement, judicial, hybrid). As regards EU FIUs that have a police or judicial nature, they all have confirmed their capacity to provide information to administrative counterparts, without impediments possibly deriving from the law enforcement purposes pursued in their activities and the nature of the powers available in these contexts[160].

A respondent has indicated that, due to the necessary protection of the confidentiality of reporting entities, cooperation cannot be provided in cases where the identity of these reporting entities would have to be disclosed; however, the same respondents also clarify that these cases only rarely occur as references to particular reporting entities can normally be deleted from FIU-to-FIU communications without losing important content for the analysis or for the ensuing investigations.

Other instances where the exchange of information can be refused by EU FIUs are based on general circumstances related to, for example, the risk of violation of human rights, national sovereignty or national interests. These instances appear to be formally in line with the correspondent provisions in article 53(3) of the fourth Directive. However, the Directive does not set out the scope of these

[160] See, however, information and considerations in previous Chapters and paragraphs on how the lack of a clear separation between law enforcement activities and analysis can affect FIUs' operations and cooperation.

exceptions in any detail and no indication is available as to how these same exceptions are spelt out in domestic regulations and practices.

As already recalled, in several cases respondents indicate that they cannot provide information (not even for FIUs' own analytical activities) if it is believed that this could affect domestic investigations or legal proceedings. Many respondents have also specified that they can only provide information for intelligence purposes and, if such information is to be used as evidentiary material in legal proceedings, then a mutual legal assistance request is needed through the appropriate police or judicial cooperation channels.

Finally, respondents have specified that cooperation is refused if the request appears to be driven by "political" motivations, rather than being based on genuine money laundering or terrorist financing suspicions.

3. Completeness of the information shared

As already noted, the range and types of the information that can be shared is one of the essential factors (together with, i.a., possible conditions for the response[161] and the capacity to use domestic powers for international cooperation purposes[162]) that have to be considered to come to an adequate assessment of the FIUs' capacity to provide cooperation to foreign counterparts. This in turn depends, as also recalled, on the extent of the FIUs' access to information at the domestic level[163]. In this paragraph the focus will be on limitations or conditions applicable to EU FIUs in transmitting particular types of information, variably grouped under the general categories of "financial", administrative" and "law enforcement". These conditions and limitations clearly affect the overall scope of the exchanges and have to be carefully considered with a view to removing existing barriers and enhancing the effectiveness of FIUs' action.

3.1 Sharing Financial and administrative information

As regards "financial" information, this is normally intended to encompass, i.a., data about financial transactions, bank accounts or other business relations with credit or financial institutions, transfers of funds, cash operations. This information may come either from STRs/SARs filed to the FIU by reporting entities or from external sources or other parties that the FIU can access or approach[164].

Based on responses to the Survey, EU FIUs are generally in a position to share financial information. In few cases some conditions are applicable. Some respondents have reiterated that this information can only be provided for intelligence purposes and cannot be used in judicial proceedings.

A respondent has explained that information is sent based on an assessment about "justification, proportionality and necessity", particularly with a view to avoiding that an excessively vast range of financial data is requested by foreign FIUs besides what is actually required by these FIUs in light of the case and the associated analytical needs.

In such cases, while legitimate data protection concerns might play a role, it is necessary to limit the risk that the requested FIU unduly reassesses the information needs that had led the counterpart to

[161] As discussed in par. 1.
[162] See par. 4.
[163] See Chapter 3 on the FIUs' access to financial, administrative and law enforcement information.
[164] The availability of "financial" information for FIUs is discussed in Chapter 3. Chapter 4 deals with the EU FIUs' capacity, and related limitations, to obtain information from obliged entities.

file the request based on its evaluation of the case and in the intent to produce an effective analytical output in support of ensuing investigations by domestic law enforcement agencies.

A respondent has flagged that only information can be shared, not the documents (or their copies) where such information is incorporated.

Respondents have also highlighted situations where financial information can only be transmitted (not directly by the FIU, but) via formal international letters of requests (ILOR), that is in a Mutual Legal Assistance context (this information includes bank account and financial transactions data). This of course amount to a significant limitation to the capacity to provide FIU-to-FIU cooperation in accordance with standards required by the Directive.

Other conditions and restrictions apply to financial and administrative information that has to be obtained from other agencies, and that the FIU may be prevented from sharing with foreign counterparts. Based on responses to the Survey, this is in some Member States the case of data on beneficial ownership, border crossing by natural persons, passport details, customs and fiscal records, export-import of goods, social security, banking and financial licenses and compliance.

As regards specifically information on particular reporting entities that have filed STRs/SARs, this is subject to a more rigorous level of protection and, for the majority of EU FIUs, it cannot be shared or can only be shared subject to additional conditions. The need to protect reporting entities and their employees from undue exposure lies at the basis of these special restrictions. These also pursue the objective of ensuring that appropriate incentives are in place for an effective and systematic disclosure to the FIU of suspicious cases.

While five FIUs are prevented from sharing information on reporting entities, other FIUs only provide this data upon a demonstrated "need to know" basis. In one case, information on reporting entities is equated to law enforcement information and can only be shared through appropriate police channels.

The survey highlights that, although many FIUs can share financial and administrative information, there are significant cases where considerable impediments and conditions continue to exist. These pertain to prohibitions to forward particular types of information (especially that obtained from other domestic entities) and also to outright lack of capacity due to the need to pursue separate law enforcement cooperation channels. These are circumstances where the requirements to exchange information, stipulated in the Directive, do not seem to be complied with. Concerns also arise on the scope of the cooperation in cases where this is made subject to an assessment by the requested FIU on the underlying case and the "proportionality" of requests.

While national implementation of existing EU provisions should be improved by enlarging and enhancing FIUs' access and capacity to exchange financial and administrative information, more detailed minimum standards in this regard should be set out at the EU level. This could, at the same time, facilitate common approaches across EU Member States as to the types of information that should be available to FIUs and to the need to dispose of this information, both for domestic analysis and for international cooperation, with no undue conditions or limitations.

More particularly, it should be clarified that (as already recalled) requests, and the underlying cases, should not be second-guessed by the requested FIU to establish the extent of the cooperation that can be provided. The information needs are set by requesting FIUs and respondents should act accordingly, based on any further clarification needed.

Another point to reinforce is that the exchange of financial information (whose scope and types, as said, should be set out in in sufficient details to facilitate uniform approaches) should always be possible through the FIU-to-FIU channels and that refusals based on the need to use the Mutual Legal Assistance designed for law enforcement or judicial cooperation should not be admitted. These limitations, as already highlighted, seem to be rooted in the absence of a clear demarcation between the analysis of suspicious cases of money laundering or terrorist financing and the investigation carried out on the same facts: while the two functions should be respectively, and separately, carried out by the FIU and competent law enforcement agencies, they can be unified in one overall process in cases where the FIU is also a police body. As also said, while this issue should be addressed through better national implementation of current EU provisions, its relevance and pervasiveness seems to suggest that a better common understanding or a reinforcement of such provisions on this point would be particularly beneficial.

3.2 Sharing Law enforcement information

The majority of EU FIUs can share law enforcement information with no particular conditions attached. However, in several cases this capacity is significantly limited. Some FIUs have indicated that, although only in exceptional cases, law enforcement agencies can impose restrictions on the exchange of police information or deny the authorization which is foreseen for this purpose (see also par. 2, where the impacts of ongoing investigations or legal proceedings on FIUs' cooperation are recalled, besides the exchange of law enforcement information). In this respect, a respondent has specified that it can provide information obtained from a police database while other operational information or inquiries to other national law enforcement agencies can only take place in a police-to-police cooperation context.

In other cases, also referred to in responses to the Survey, law enforcement information cannot be provided directly by the FIU but has to be requested through separate mutual legal assistance channels of cooperation. Some respondents have indicated that, due to the need to approach other agencies to obtain law enforcement information, this is based on an ad-hoc agreement between the FIU and such agencies (that only allows the FIU to access a set of basic data on types of offences and dates of criminal reports) and requires an extended period of time, during which the foreign request remains pending. In one case, in order to obtain police information, the FIU has to share the content of the counterpart FIU's request with competent law enforcement agencies; for this purpose, the prior consent of the requesting FIUs has to be obtained, which also implies lengthy procedures and an extended response time[165].

Finally, it is worth noting that a police FIU has flagged that, due to data protection restrictions, it cannot provide information on account statements and criminal intelligence to FIUs that have an administrative nature.

These limitations, particularly diverse in nature and effects, are susceptible of affecting FIUs' capacity to access and share law enforcement information. The requirements under articles 32(4) and 53 of the fourth Directive, that envisage that FIUs should freely dispose of and exchange, i.a., law enforcement information[166] does not seem to be fully or properly implemented in all cases. Two concurrent factors seem to lie at the basis of existing problems for EU FIUs to exchange law

[165] In this particular case, it is also important to stress that, while the FIU has a duty to provide, i.a., law enforcement information, this duty cannot be made subject to the previous sharing of the request and of the underlying case with competent domestic law enforcement agencies. More particularly, law enforcement information should be provided also in cases where the requesting FIU does not allow for its request, and the information contained in it, to be shared with such agencies.

[166] See also the explicit reference in article 4(2) of Council Decision 2000/642/JHA.

enforcement information.

On the one hand, EU FIUs encounter significant limitations and difficulties in accessing law enforcement information at the domestic level. These limitations and difficulties are essentially twofold: a) the range of available or accessible law enforcement information is often particularly narrow (for example, investigations or legal proceedings which are currently underway may remain unknown to FIUs, especially administrative ones, in the course of their analyses); b) the procedure to access this information is often indirect and entails approaching or liaising with third parties with limited possibilities for direct enquiries to databases by the FIUs (the features and limitations of FIUs' access to law enforcement information domestically are more amply discussed in Chapter 3).

On the other hand, law enforcement information available to FIUs, besides being often partial or incomplete, is also frequently subject to conditions in its exchange with foreign counterparts; the FIU may need a prior authorisation for this purpose from the domestic law enforcement body owning and providing the information.

Along the lines of previous considerations about the access to and the sharing of financial information, while Member States should ensure a better implementation of the EU provisions on this matter by allowing FIUs to access and exchange police information more broadly and swiftly, further and more specific details could be provided in EU legislation. This could, for example:

- specify the law enforcement information that, as a minimum, FIUs should be able to access and share; data on past criminal records, ongoing investigations or legal proceedings, provisional measures, seizures, confiscations, could for example fall into this scope;
- explicitly prohibit undue limitations or conditions, particularly in the forms of cumbersome access procedures at the domestic level or needs to obtain authorisations from third parties; possible caveats and exceptions may of course apply in cases of ongoing investigations or prosecutions, although instances where forwarding police data to an FIU for its internal analysis is likely to jeopardise law enforcement operations can be hardly imagined.

4. Use of domestic powers to respond to requests from other EU FIUs

In line with FATF standards, the fourth Directive establishes that FIUs should not only share information already available to them (typically that coming from STRs/SARs or gathered through previous analyses) but should also be able to obtain any further information needed to provide the counterpart with the requested cooperation. For this purpose, FIUs should be empowered to exercise their own domestic powers, the same they would have used to carry out the analysis had the case to which the request refers to been reported to them. In fact, under article 53(2) "Member States shall ensure that the FIU to whom the request is made is required to use the whole range of its available powers which it would normally use domestically for receiving and analysing information".

This entails that requests from other EU FIUs are equated to domestic STRs/SARs for the purpose of activating the powers available to perform analysis and obtain information. According to the Directive, the "whole range" of domestic powers must be also available for international cooperation. This of course does not imply that all powers have to be activated for each request, regardless of the case. Rather, the requested FIU is expected (and should be empowered

accordingly) to exercise those powers in its toolkit which are needed to gather the information that is requested or is otherwise relevant to respond to the enquiry in light of the case[167].

Another way to look at the equation between foreign requests and domestic analyses is that suspicious cases submitted by EU FIUs through requests for cooperation are mutually "recognised" as equally relevant by the requested counterparts, which as a consequence are empowered and required to act on them as if they were reported or identified domestically.

The effect of this innovative rule on FIU-to-FIU cooperation is therefore a significant increase in the range of information available for international cooperation. This range becomes strictly dependent on the scope of the information powers attributed to FIUs by their respective national legislations. These powers are particularly diverse across Member States, in the absence of sufficiently harmonised provisions in the fourth Directive; consequences of this diversity and lack of harmonisation will be recalled later on in this paragraph, also in light of comments provided by respondents.

4.1 Legal basis (at national and EU level) to use domestic powers

Responses to the Survey indicate that the requirement for FIUs to use their domestic powers to obtain and share information with other EU counterparts is already widespread across Member States. Only one FIU has reported that this is not allowed under its domestic law. However, it appears that this requirement is not always specifically and explicitly reflected in laws or regulations. The FIU's capacity to use its domestic prerogatives to obtain information on behalf of foreign counterparts may in several cases be based on the relatively broad formulation of general provisions which empower FIUs to access information for their own general purposes, in such a way as to allow (often implicitly or indirectly) to use these powers and the information that can be obtained also to provide cooperation to foreign counterparts.

There is no requirement for Member States to have provisions in place which explicitly and specifically require or allow their FIUs to use domestic powers for FIU-to-FIU cooperation purposes. What is important is that national legal bases, as implicit as they may be, are nonetheless fully clear and sufficiently robust so as this objective can be unequivocally achieved, in line with the fourth Directive. However, enacting targeted national provisions might be appropriate to establish beyond any possible doubt that the range and scope of the FIUs' powers are extended beyond the domain of domestic analysis and cover also FIU-to-FIU cooperation and that, based on this, the FIU is at the same time empowered and required to deploy such powers to gather information on behalf of other EU FIUs.

In this regard, some respondents have in fact highlighted that, while there is no restriction to the use of available powers, an explicit requirement mirroring that in article 53(2) of the Directive is absent in their legal frameworks.

Several others point out that, more than a requirement stipulated in national law to cooperate in accordance with article 53(2), the FIU is only empowered to do so (thus it is not clear if available powers can be, and are in fact, used in all cases in international cooperation contexts).

[167] It is important to recall, again, the possible implications on this delicate aspect of the principle of reciprocity: FIUs may refrain from using those powers which, although relevant to respond in that particular case, they have reasons to believe the requesting counterparts would (or could) not use if requested under similar circumstances.

In such situations, more explicit and detailed national provisions empowering and requiring FIUs to use domestic powers also for cooperation purposes may be appropriate to ensure an adequate implementation of the Directive on this point. These provisions should more firmly root this requirement into the FIU's toolkit and range of activities, against any possible doubts as to whether the FIU is enabled and required to exercise available powers for international cooperation purposes, as well as to address legitimate concerns related to data protection safeguards and as to whether these should prevail over the duties to share information with foreign counterpart (thus limiting this sharing).

National provisions may also be appropriate to determine the extent to which domestic powers should be exercised to respond to foreign requests, for example by clarifying that the FIU has certainly a duty to exhaust all available means to provide the information needed but that not all the information powers should be activated in all cases, as they should rather be proportionate and calibrated in light of the case and in accordance with the information needs specified by the requesting counterparts.

Common and uniform indications in this regard could also be set out at the EU level. This would not only provide guidance and a framework for this important aspect of FIU-to-FIU cooperation (as also flagged by some respondents) but would also limit discrepancies and differences among FIUs capacity to access and share information.

These discrepancies, already particularly pronounced in the current framework, will become even more prominent when the fourth Directive will be fully implemented by all Member States, precisely due to the requirement to use domestic powers, diverse in nature and extent, for international cooperation. In fact, as already noted and as also recalled by several respondents, differences in this area can have adverse effects on FIUs' cooperation which would easily propagate via the application of the principle of reciprocity.

The adoption of more detailed common provisions or guidance at the EU level would mitigate such undesired effects which could potentially set off the benefits brought about by this new requirement.

An important additional remark put forward by several respondents concern the need, in order to be able to exercise domestic powers for obtaining information, that requests be particularly specific as to the motivation, describing the case and the associated information requirements in sufficient details. This "reinforced motivation" is reported in many cases as particularly important to allow the requested FIU to approach other agencies from which the information has to be obtained, which in turn may ask the FIU for appropriate motivation.

4.2 Scope of available powers and existing limitations to their exercise on behalf of foreign FIUs

As regards the scope of EU FIUs' capacity to obtain and share information by making use of domestic powers (which, as said, vary considerably across Member States), responses to the Survey confirm that this in general includes both the possibility to perform queries into external databases or other agencies and the acquisition of information from domestic obliged entities.

As regards external queries, responses show that these are in some cases subject to conditions, mostly related to the types of information (as some can only be transmitted through police channels), to the agencies that have to be approached (as not all can allow their data to be shared with foreign FIUs through the FIU-to-FIU channels), to authorizations that are foreseen by these

authorities, to the prohibition to obtain and share tax-related information and, again, to the condition of reciprocity.

As regards the capacity to obtain information from obliged entities where needed to respond to foreign requests, this is generally available to EU FIUs. One respondent has explicitly indicated, though, that its current domestic legal framework does not allow to exercise this prerogative. The ability of EU FIUs to obtain information from obliged entities is specifically discussed in Chapter 4, where existing conditions and limitations are also recalled.

General limitations. The same limitations and conditions that in general affect FIUs' capacity to provide cooperation also apply when it comes to exercising domestic powers to obtain information which is destined to international sharing. Such conditions are related to the lack of power by the FIU to obtain information, to the need to use police international communication channels, to filters based on adequate "justification" and on proportionality between the request and the underlying case. Responses confirm that the conditions and limitations which still affect FIUs' cooperation in general (see especially par. 2) also apply to the exercise of domestic powers to obtain and exchange requested information.

Prior STRs/SARs. Consistently with the findings recalled in Chapter 4, some FIUs have indicated that they can obtain information from domestic obliged entities only when an STR/SAR has already been reported by the relevant obliged entities on the same case. In cases where relevant STRs have not been filed, the requested FIU cannot obtain information on behalf of foreign counterparts and, as a consequence, cooperation cannot be provided.

Banking and financial information. Other restrictions are encountered by FIUs, based on the responses to the Survey, as regards the capacity to obtain and share banking and financial information (such as data on bank accounts and transactions). Lack of access to financial information, similarly to domestic analysis, equally affects FIUs' capacity to provide this information to foreign counterparts in the contest of FIU-to-FIU cooperation.

Investigations or legal proceedings. FIUs' capacity to use domestic powers to obtain and share information is also inhibited in several cases when investigations or legal proceedings are underway on the same matters. Responses indicate that these limitations range from outright prohibitions to the need to obtain authorizations from competent law enforcement agencies or prosecutors.

Predicate offences. Similarly, some respondents confirm that their FIUs cannot obtain information and share it with foreign counterparts if the (possible) predicate offence underlying the case to which the request refers is not indicated or, when indicated, it is not criminalised in the same form under domestic law. This constraint seems to play a particularly prominent role in this context: in fact, some FIUs have indicated that they need stronger motivations and more compelling reasons, clearly demonstrating the underlying criminality for proportionality considerations, in order to be able to reach out to external sources of information compared to what is sufficient for sharing information which is already available.

Responses also highlight that, often, a case-by-case assessment has to be done by the requested FIU to ascertain whether a predicate offence is clearly delineated in the request and if this offence is also criminalised in domestic legislation.

This scrutiny, although still applicable in order to verify if forms of criminality are properly indicated in the requests, is alleviated for those FIUs whose legal systems adopt an "all crime" approach to the definition of the scope of predicate offences for money laundering. Respondents in

fact have indicated that in such cases they do not need to perform an assessment on the predicate offence being criminalised precisely "in the same form" domestically, being sufficient to verify that it is indeed covered by the national criminal law framework.

As already noted (see esp. par. 2.2 and par. 2.3), these forms of conditionality imposed on FIUs' capacity to exchange information for their analytical purposes, appear to be based on an inappropriate super-position of different and separate dimensions, that is the analysis of suspicions and the ascertainment of crimes. Blurring this essential distinction, which is at the basis of the FIUs' definition and *raison d'etre*, goes to the detriment of FIUs' administrative cooperation for analytical purposes, as this is made dependent on (and subject to) criminal law considerations.

In any event, as also noted earlier, limitations based on the identification and nature of predicate offences go against the fundamental rule of "free exchange of information for analytical purposes", set out in article 53(3) of the Directive. In line with previous proposals[168], the EU legislation on this point should be made unequivocal and reinforced.

More in general, the limitations which, according to the responses, significantly limit the FIUs' capacity to make use of their powers to obtain information on behalf of foreign counterparts do not seem in conformity with the fourth Directive (specifically, with the requirement spelt out in article 53(2)). While FIUs' seem to rely in several cases on general provisions empowering them to access domestic data sources, dedicated implementing provisions are needed for a proper and unequivocal transposition of these EU provisions, allowing (and requiring) FIUs to exercise these powers also to provide cooperation to foreign FIUs.

At the same time, as already recalled, more specific indications at the EU level would also be helpful to ensure a common understanding and a uniform approach across EU Member States and FIUs on the extent of the duty to provide cooperation and on the need to avoid that this is unduly constrained by domestic conditions.

In accordance with the need for reinforced motivation in order for FIUs to be able to activate their own powers to obtain information needed for international sharing, the majority of respondents have indicated that, for this purpose, requests have to set out an adequate description of the case subject to analysis and of the associated grounds for suspicion. Where requests are not adequately substantiated, requested FIUs may not be in a position to obtain information by making use of their domestic powers.

There is a risk that FIUs may exercise considerable discretion in assessing the case and the merits of the suspicion, refusing to use their powers to gather requested information (thus denying cooperation, in all or in part) if they deem the request as not sufficiently substantiated, the suspicion not adequately founded or simply the case not sufficiently "serious" (for example, due to the type of the predicate offence). This risk seems heightened by the large level of discretion that in many cases Member States' legislations seem to confer upon FIUs in this context (see also previous considerations on the domestic legal basis transposing article 53(2) and the generic/implicit approach that has been adopted in some Member States to empower FIUs to use domestic powers for FIU-to-FIU cooperation purposes).

Clearly, the capacity to second-guess the relevance of the case and the merit of the underlying suspicion may go against the principle of "mutual recognition" of suspicions among EU FIUs and the associated requirement for EU FIUs to use their domestic powers to lend the requested

[168] See par. 2.3.

cooperation. On this note, some respondents have specified that, while they require adequately motivated requests to activate own powers, the counterparts' grounds for suspicion is not re-assessed or second-guessed.

In any event, there seems to be a delicate balance to be struck between the need for appropriate motivation (and the consequent right for the requested FIU to be fully appraised of all relevant facts) and the assessment of requests for the exercise of domestic powers to gather information.

The considerations developed above on the need for appropriate clarifications through provisions or guidance at the EU level on the relations between the obligation for the requesting FIU to file properly motivated requests and the duty for the requested FIU to provide cooperation should be recalled here. As discussed, the motivation in the request is intended not to allow the requested FIU to second-guess the request but rather to provide targeted assistance in conformity with the counterpart's needs. Poorly motivated requests should trigger a dialogue between the FIUs involved and should not justify a refusal to provide cooperation.

On a positive note, with very limited exception, respondents have not reported the existence of conditions or limitations as regards the capacity to apply domestic powers to exchange information with FIUs that have different nature or status. Police or judicial FIUs have indicated that they can provide these forms of cooperation to respond to requests from administrative counterparts, and vice versa.

5. Cooperation in cross-border cases

5.1 Cross-border STRs/SARs

Article 53(1), third paragraph, of the Directive introduces a new requirement for EU FIUs and their cooperation: besides the provision of information which is done on request from other FIUs or spontaneously (article 53(1), first paragraph), EU FIUs have now an obligation to "promptly forward" to the interested FIUs every STR/SAR "which concern another Member State".

Differently from responses to foreign enquiries, these disclosures are not dependent on requests filed by other FIUs. Also, differently from spontaneous sharing, the forwarding of STRs/SARs that "concern another Member State" is a mandatory feature under article 53 of the Directive. This is therefore an innovative obligation for FIUs, consisting in automatic and compulsory forms of disclosure.

It is also important to note, in light of the information and comments provided by respondents (see below), that this obligation of automatic disclosure is unconditional and, more particularly, not limited on the basis, for example, of the judgement of the obliged FIU or on the outcome of its analysis. The obligation to forward applies to any received STR/SAR based on the sole objective condition that it "concerns another Member State".

As regards the scope of such obligation, this is left undetermined in article 53 and is therefore potentially very broad. Equally broad is the potential impact of its implementation on EU FIUs: as respondents have flagged, depending on how the notion of STRs/SARs concerning other Member State is interpreted, EU FIUs may be required to transmit and receive sheer amounts of disclosures, with several practical implications and an increase of the operational burden and of the workload. Based on the mandate assigned to it by article 51 of the fourth Directive, the EU FIUs' Platform can provide advice and criteria on, i.a., "the identification of suspicious transactions with a cross-border dimension".

In any event, forms of information-sharing among FIUs on suspicious activities that have a cross-border nature and, therefore, may concern Member States other than the one of the FIU receiving the disclosures are essential to make sure that information on suspected money laundering or terrorist financing activities is provided to those FIUs that are best placed to act on them, particularly in cases concerning potential criminal activities committed in their territories.

As a consequence of the peculiar territorial criterion underlying the AML/CFT obligations in general and the duty to report suspicions in particular, STRs/SARs have to be transmitted "to the FIU of the Member State in whose territory the obliged entity transmitting the information is established"[169]. This applies also in cases where the reported suspicious transactions are performed by the reporting entity in another Member State (or in a third country), as is typically the case of entities operating abroad under the free provision of services regime. In such circumstances, the FIU of the Member State where the potential money laundering or terrorist financing takes place does not receive the STR/SAR and, on the other hand, the FIU of the country where the reporting entity is established is not in a position to act effectively on the received STR/SAR as this concern activities that occur outside of its territory.

The mechanism for mandatory information devised in article 53(1), third paragraph, of the fourth Directive addresses this "asymmetry" in the distribution of information by requiring the FIU that receives the disclosures of a such cross-border nature to forward them to the FIUs of the countries involved in the reported transactions.

5.1.1 Legal basis for sharing cross-border STRs/SARs

Faced with this innovative obligation to provide international cooperation, the majority of EU FIUs have indicated in their submissions that, under their respective domestic legal frameworks, they have the capacity to forward disclosures which concern another Member State to the FIU of that Member State, in accordance with article 53(1) of the Directive. Only one respondent has clarified that the legislation needed to implement this requirement has not been enacted yet.

However, based on responses to the Survey, it appears that in the vast majority of cases, FIUs' capacity to share "cross-border STRs" does not derive from newly adopted provisions specifically transposing article 53(1) for this part. In fact, many responses specify that domestic implementing provisions are still lacking and that disclosures of information related to cross-border STRs are carried out by means of the general capacity to provide information spontaneously (as foreseen by a different provision in the same article 53(1) of the Directive). Most importantly, respondents indicate that they rely for this purpose on their capacity to provide information to other EU counterparts on a spontaneous basis, that is upon own initiative and in the absence of ad-hoc requests.

This cannot be considered sufficient to meet the requirement under the fourth Directive on the sharing of cross-border STRs/SARs, particularly because, as said, the sharing of disclosures that concern other Member States is, under the Directive, an outright obligation for FIUs, not a spontaneous and, as such discretional initiative of interested FIU.

[169] See article 33(2).

5.1.2 Conditions and limitations to the sharing of cross-border STRs/SARs

Moreover, while as said the obligation to forward "cross-border" STRs/SARs is not subject to conditions under the Directive, several types of filters are currently applied by FIUs, as clearly described in their submissions on this point.

More than half of the respondents have confirmed that cross-border STRs/SARs are not systematically shared and are rather filtered based on a number of different criteria. The assessment is often done on a case-by-case basis, exercising ample discretion and with no particular reference to objective factors determining when a disclosure may concern other Member States.

For example, respondents highlight that they can proceed to this spontaneous sharing when it is deemed "necessary" or "relevant", when there are relevant "grounds for suspicion" (beyond those that have pushed the reporting entity to file the disclosure) or following an evaluation of proportionality which takes also account of the identification of adequate suspicions of criminality in the interested Member State.

Generally, responses to the Survey also highlight that, in many cases, the sharing is done, rather than upfront upon the receipt of relevant disclosures from domestic reporting entities and based on objective or automatic criteria, only after appropriate analysis and subject to the findings of such analysis.

According to the responses, these filters are also applied to ensure a selection of disclosures necessary to avoid that massive amounts of data and volumes of STRs/SARs be circulated across Member States, thus managing the impact of this provision and keeping this task feasible.

Potential obstacles to the system of automatic disclosures of cross-border reports seem also to arise from constraints at national level that prevent FIUs from forwarding information without a prior "validation" through analysis (or investigation) which confirm that the case is properly substantiated.

In this respect, a respondent has flagged that the STR/SAR received "is only 'information': it has come from a non law enforcement source and contains uncorroborated facts. It does not become intelligence until it has been assessed and checked against other databases, and then agreed to contain a reasonable suspicion of link to crime or terrorism". The concern is that the FIU "would surely be breaking Human Rights law (right to privacy)" if cross-border STRs/SARs were "sent on to the other MS mentioned without a possible link to crime or terrorism being established. The mere suspicion of the reporter is not sufficient, there has to be an informed/ second opinion view formed".

In addition to specific filters applicable to the particular matter of circulation of cross-border disclosures, all general conditions and limitations that for many FIUs restrain the capacity to provide cooperation apply in this area as well. Similarly to what has been described in previous paragraphs for other aspects of FIU-to-FIU cooperation, information on STRs that have a cross-border dimension and concern other Member States may not be shared with relevant FIUs (in all or in part) in situations where the underlying criminal offence cannot be determined (by the FIU that has received the disclosure from the reporting entity) or is not criminalised domestically, regardless of whether or not it may constitute a criminal offence in the Member State where the suspicious activity has taken place.

Also, due to domestic restrictions, bank and financial information contained in cross-border STRs/SARs cannot be shared in some cases. The sharing can also be inhibited or conditioned by the existence of investigations or legal proceedings on the same case (in the country of the FIU that has received the disclosure from the reporting entity). Also due to general domestic restrictions to information sharing, some FIUs are prevented from forwarding cross-border STRs/SARs that are connected to tax matters or involve tax information.

As regards practical difficulties associated with the application of the cross-border STRs sharing, a respondent has also referenced issues concerning the language of the disclosures. These are of course filed in the language of the country of the receiving FIU (that is, the country where the reporting entity is established) and the question arises if, at least in some cases, a translation should be carried out into English or into the language of the FIU to which the disclosure has to be forwarded (this would of course add on to the difficulties associated with this new requirement).

As said, the requirement to forward disclosures that concern other Member States, as stipulated in article 53(1) of the Directive, were not implemented specifically in the vast majority of EU Countries at the time when the survey was carried out. It is therefore perhaps too early to evaluate where EU FIUs stand with regard to the practical application of this innovative requirement. It is hoped that the limitations and conditions highlighted by respondents will be addressed and solved through appropriate domestic transposition.

The obligation to forward cross-border STRs/SARs needs to be properly implemented in Member States based on appropriate legal bases. Existing provisions empowering FIUs to share STR information spontaneously with foreign counterparts is not sufficient to satisfy this new requirement. In fact, the communication of disclosures that concern other Member States is a mandatory task which should not depend on a spontaneous initiative of the FIU that so decides on a case-by-case discretionary decision.

It is also important that the requirement to forward cross-border STRs/SARs is transposed into national legislations as an unconditional obligation for FIUs. In accordance with the Directive, these 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.

On how to ensure that the provision about sharing cross-border disclosures is implemented properly and uniformly, at least two sets of comments formulated by FIUs stand out.

- In the absence of a definition in the Directive of STRs/SARs that "concern another Member State", there is certainly a need to specify the scope of this obligation by setting out appropriate criteria in applicable laws or regulation. This is particularly important given the extremely wide range of instances which may fit the description and the potential impact on FIUs' exchange and sharing activities, as well as on domestic analytical functions.

- It would be clearly appropriate, and even necessary for the implementation and practical application of this provision, if more detailed indications and criteria to determine when an STR/SAR may qualify as having a "cross-border" nature were defined at the EU level, so that discrepancies can be avoided in the application of this EU-wide obligation. This would

at the same time facilitate legal and practical implementation and avoid (or limit) unjustified discrepancies among national approaches[170].

These criteria have to be set having in mind, on the one hand, the need for sharing actionable disclosures, which is the driver that inspires the requirement in article 53(1), third paragraph, to remedy the gaps and asymmetries caused by the territorial criterion for the reporting obligation, as recalled above.

On the other hand, appropriate criteria should result in an exchange regime which is manageable, in light of the potentially massive amount of STRs/SARs that may be considered to qualify as of "interest" for other Member States, with significant implications for both the sending and the receiving side (the two of course normally coexisting in each FIU, although the proportion between them may vary across countries). Several respondents have flagged this aspect as one of the most relevant in the implementation of the new EU AML/CFT framework, indicating that, depending on how this implementation will be realised, significant feasibility and resource implications may arise for FIUs.

Finally, as for other forms of FIU-to-FIU cooperation, the conditions that limit the capacity to share cross-border STRs should be removed (as noted, this is the case for example of the existence of criminal investigations or legal proceedings or STRs concerning tax matters or information). EU rules would be helpful to unequivocally clarify and effectively achieve this objective.

5.2 Obtaining and forwarding information from obliged entities established in the territory of the requested FIU and operating in another Member State

For the analysis of cross-border disclosures which concern another Member State, sharing such disclosures with relevant FIUs is not sufficient: it is also necessary to ensure that these FIUs can obtain additional information from the reporting entities, whenever this is needed for the analysis. This is what article 33(1) of the fourth Directive aims at achieving, under ordinary circumstances, by assigning FIUs the power to request and obtain this additional information from obliged entities established in their respective territories. However, article 33(1) is not applicable to the case of cross-border STRs/SARs, due again to the territoriality criterion underpinning AML/CFT obligations: the power to obtain information, in fact, is not applicable to entities which are not established in the territory of the interested FIU. In the absence of ad-hoc provisions, the FIU that

[170] One important underlying problem lies in the differences among the very notions and contents of STRs/SARs across Member States. Common criteria can be defined on when a disclosure has a "cross-border" nature but this would not overcome the differences as to what an "STR/SAR" is under Member States' national frameworks in the first place.
This is also an area where the Directive lacks details, leaving ample room for widely different national approaches. These differences are reflected in FIUs' analytical functions and outputs, which are of course dependent on the information collated through STRs/SARs, as well as on the volume of such disclosures, also very diverse across Member States and in turn dependent on the domestic scope and notion of "STR/SAR". Moreover, these differences have a significant impact on FIUs' cooperation, which is also based on the information contained in the disclosures received, particularly when it comes to sharing STRs/SARs that, despite their cross-border relevance, remain diverse in their structure and information content and may not fit the analytical needs and practices of the FIUs of the Member States "concerned", under the meaning of article 53(1). For example, STRs/SARs filed in a Member State may be triggered by the detection of possible predicate offences, before actual proceeds (and the related money laundering) generated by these offences are identified or regardless of such proceeds. These kinds of disclosures, focused on the predicates rather than on the subsequent money laundering, may not even be actionable by the FIU of the "Member State" concerned to which they are forwarded.
These discrepancies among the contents and nature of STRs/SARs in different Member States may well extend to the inception and conduction of "joint analyses" which, as discussed in par. 8, focus specifically on activities that have a cross-border dimension and benefit from forms of cooperation among FIUs beyond the exchange of information (article 51 of the fourth Directive).

receives cross-border STRs/SARs forwarded by a foreign counterpart could not obtain information from obliged entities established in the country of origin of the disclosure.

Therefore, to fulfil these information needs the cooperation of the FIU of the country where the "obliged" entity is located is also necessary, under a mechanism similar to that designed for the forwarding of cross-border STRs. This mechanism is consistently provided for under article 53(2), second paragraph: "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". Therefore, further to the obligation to share cross-border STRs/SARs, the FIU of the country of establishment of entities operating abroad has also an obligation, upon request by the interested EU FIUs, to obtain and provide additional information from such obliged entities and forward it to the foreign counterparts concerned.

The majority of EU FIUs have indicated that they have the capacity to respond to such requests. There are however two exceptions where this form of cooperation cannot be provided due to the absence of a legal basis.

Nonetheless, similarly to what has been observed for the duty to forward cross-border STRs/SARs, it seems that this requirement is also implemented through the same general provisions empowering EU FIUs to obtain information from obliged entities and to exercise this power also to respond to requests from foreign counterparts. In other words, based on these responses, the legal basis that EU FIUs are apparently using to obtain on behalf of foreign FIUs additional information from obliged entities established in their territory and operating in another Member State, following cross-border disclosures, is that corresponding to articles 32(3) and 53(2) of the Directive, rather than that under article 53(2), second paragraph, specifically introduced for this particular purpose.

In any event, differently from what has been observed in the previous paragraph for the forwarding action, which is based on general domestic provisions about spontaneous disclosures rather than on a dedicated legal basis setting out a mandatory requirement, the Directive provides for an obligation for FIUs to obtain information from obliged entities on behalf of requesting EU FIUs[171]. This general obligation, if properly implemented by Member States, should in principle cover all cases where foreign FIUs request information held by obliged entities, including those, separately envisaged in article 53(2), second paragraph, of the Directive, regarding the specific case of entities operating abroad and related cross-border STRs/SARs.

Nonetheless, although the general FIUs' power to obtain information from obliged entities might encompass also cases of entities operating abroad and the sharing of that information with other FIUs as a follow up to cross-border disclosures, a specific and targeted implementation through appropriate national provisions specifically addressing this particular duty of cooperation in cross-border situations would reassure about the correct transposition and the effective implementation by EU FIUs. This seems needed also to overcome the usual conditions and limitations that, similarly to other aspects of FIU-to-FIU cooperation, affect this particular instance of exchange of information.

In this regard, in fact, some respondents have confirmed that information cannot be obtained from obliged entities and, therefore, requests from foreign FIUs for this information are declined or delayed, where there are no previous STRs/SARs reported domestically on the same case[172], or the

[171] Article 33(1)(b) and article 53(2) of the Directive.

[172] Luckily, as said, article 53(2), second paragraph, of the Directive is normally triggered following cross-border STRs/SARs reported to the requested FIU and forwarded to the requesting FIU, so that this condition can be satisfied.

predicate offence is not determined or is not criminalized, certain types of financial or fiscal information are involved, investigations or legal proceedings are underway in the country of the requested FIU.

6. "Known/Unknown" exchanges

In addition to ordinary exchanges based on motivated requests (article 53(1), second paragraph) the Directive also envisages "different mechanisms" which may be applied "if so agreed between the FIUs". This provision explicitly mentions the "exchanges through the FIU.net or its successor". The reference here, although not explicitly made, is to "known/unknown" types of exchanges: those are typically carried out by EU FIUs through the FIU.net; they are based on the simple indication, in the requests, of identity data of individuals and are simply aimed at determining if that data is also present in the database of the requested FIU, which means that those individuals have been reported through STRs/SARs or have been otherwise involved in analytical activities.

These "yes or no" feedbacks allow the requesting FIU to establish upfront if information is available to the counterpart approached. Neither the description of the underlying case, together with the links to the country of the requested FIU, nor the grounds for suspicion are disclosed in "known/unknown" requests at this initial stage. Requested FIUs, from their side, only provide a response indicating whether the identity data provided matches data in their own databases. Only if the reply is positive ("Known"), a properly motivated request is filed in a second phase. These exchanges, limited in the content of both the request and the response, allow efficiency gains through a better capacity to target motivated requests (which are more resource and time – consuming) only in cases of positive "hits".

The vast majority of respondents have confirmed that they can engage in "Known/Unknown" exchanges and respond to requests lacking motivation which are specifically filed with the intent to obtain feedback on whether particular subjects have been reported in STRs/SARs (or are otherwise present in the databases of the requested FIU). One EU FIU, though, has indicated that it lacks this capacity to respond to requests deprived of description and motivation.

While in most cases responses are limited to a feedback on the existence of STRs/SARs where the requested subject is mentioned, some respondents highlight that they can provide broader responses: these may include hits in other databases held by the requested FIU or even in external information sources which the FIU can access (including police databases). A respondent also recalls that, "in case of 'known' replies, the [FIU] normally invites the counterpart to file a motivated request, thus sharing the case".

Since "Known/Unknown" exchanges are carried out in derogation to the general rule that establishes that requests must be motivated, FIUs should be allowed to entertain this form of cooperation based on an appropriate legal basis (particularly in order to justify this sharing of data, though limited to "yes or no" replies, also in light of data protection concerns).

It is not clear, though, if the capacity to respond to requests bearing no description or motivation, although limited to a "hit/not hit" feedback is rooted in national laws specifically authorizing the FIU or, rather than from an explicit empowerment, this capacity is simply derived implicitly from the absence in these laws of prohibitions to proceed in this respect. An explicit legal basis allowing

the FIU to engage in "Known/Unknown" exchanges might be appropriate to overcome possible uncertainties associated with, for example, data protection concerns, as mentioned[173], or constraints related to "proportionality" which, as seen, in some cases lead FIUs to decide whether, and to what extent, a response should be provided "weighing" the substance and importance of the underlying case (which, of course, in "Known/Unknown" exchanges is not referenced).

7. Matching of data sets

Another innovative feature of FIUs' cooperation brought about by the fourth Directive is the obligation for EU FIUs to apply "state of the art technologies" (this obligation is however somehow mitigated by the clause "in accordance with their national law") allowing "to match their data with that of other FIUs in an anonymous way" (article 56(2)). This anonymous matching of data has to go along with "full protection of personal data" and aims at "detecting subjects of the FIU's interests in other Member States and identifying their proceeds and funds".

The reference in article 56(2) is also to "matching" tools developed in the context of the FIU.NET to facilitate and broaden FIUs' exchanges and cooperation. Similarly to the "Known/Unknown" exchanges, the data matching results in "yes or no" responses, depending on whether or not some of the same subjects are present in the data sets shared by the FIUs involved (following secure protocols ensuring that these data sets are anonymized).

Differently from the "Known/Unknown" exchanges, the matching encompasses multiple subjects through massive enquiries. It is based on the sharing of anonymous data and there is not a distinction between a "requesting" and a "requested" FIU. Also, the FIUs involved are not normally aware of links between particular subjects and other Member States (as the matching is carried out precisely to identify these possible links, not known in advance) and, precisely for this reason, "matching" exercises are normally conducted on a multilateral basis, so that the involvement of more than one counterparts increases the likelihood to identify links with foreign jurisdictions that can provide relevant leads for the analysis.

Positive "hits" are similar to "known" feedbacks in "Known/Unknown" exchanges but bring more information, as the FIUs involved were not aware in advance of the link with other jurisdictions. These positive results can be followed up by the FIUs involved in the matching exercise through ordinary motivated requests and comprehensive responses, in accordance with general rules.

In order to fulfil the requirements in article 56(2) about the capacity to participate in matching exercises, FIUs must have both an adequate legal basis allowing them to share data sets in anonymous forms (that is, beyond traditional request-response exchanges or even "known/unknown" exchanges related to particular subjects and particular cases) and the capacity to implement the tool in practice by making use of "state of the art technologies" made available through the FIU.NET.

Several respondents have indicated that they do not have the legal capacity, based on domestic legislation, to share in an anonymous way entire data sets extracted from own STRs/SARs databases to identify matches with other EU FIUs. Consistently, many FIUs have reported that, as a matter of fact, they do not use the matching tools provided by the FIU.NET system to identify matches in shared data sets.

[173] These concerns may arise particularly in cases where "Known/Unknown" requests are filed on multiple subjects, involved in one or more cases.

While in some cases data protection concerns (also in relation to the actual anonymity of the procedure) seem to play an important role in preventing EU FIUs from participating in matching exercises through the FIU.NET, it is important that this requirement under article 56(2) of the Directive be implemented by setting an appropriate domestic legal basis. This is precisely what some respondents mention, anticipating that future implementing legislation enacted domestically will allow to use the FIU.NET matching functionalities.

Based on developing practices, and on the overall legal framework that will result from national transpositions of the Directive on this point, the need for common guidance or provisions at the EU level might be considered. These may be needed particularly to ensure that matching tools (currently under-utilised) are routinely applied by EU FIUs, are rooted in unequivocal legal bases and are supported by a technology that fully meets appropriate effectiveness and confidentiality requirements.

8. Joint analysis

8.1 Nature and purpose

The new framework set out by the fourth Directive for FIU-to-FIU cooperation includes, among its several innovations, a reference to the conduction of "joint analyses", in relation to "cross-border cases" (see article 51). Cases that involve multiple jurisdictions become frequent and increasingly significant, also due to the activities performed by obliged entities on a cross-border basis. These may include, for example, those conducted by financial groups or conglomerates operating in different Member States[174] as well as activities carried out abroad by obliged entities under the free provision of services regime.

In these instances, besides potential difficulties in determining to which FIU suspicious transactions have to be reported (for example, in cases of operations articulated in different EU Countries or for groups that have establishments in different Member States, each being an obliged entity in its own right but being only one part to the overall activity), it may well be the case that the FIU which receives the disclosure is not in a position to obtain a full picture of the anomalous activities and perform effective analyses on its own, that is under a stand-alone approach that only relies on its information, received or accessible, and evaluations through analysis. These challenges arise at multiple levels and the fourth Directive employs a multi-pronged approach to facilitate detection and analysis of cross-border cases.

As regards the detection phase, the particular issue of how cross-border STRs should be reported to the FIU of the country of establishment and how this latter should forward such disclosures to the other interested FIUs (article 53(1), third paragraph) has already been dealt in par. 5. As said, this new cooperation mechanism aims at remedying the asymmetries in the distribution of information among FIUs that can act upon suspected money laundering or terrorist financing cases (that is, those carried out in their respective territories), deriving from the territorial criterion underpinning the STR reporting obligation. In addition, par. 5.2 deals with the cooperation mechanisms that have

[174] Interestingly, the fourth Directive makes it an explicit obligation for banking and financial groups to apply a group-wide approach (which, for multinational groups, entails a cross-border approach) to the implementation and compliance with AML/CFT measures, including as regards the identification and reporting of suspicions: under article 45, "Member States shall require obliged entities that are part of a group to implement group-wide policies and procedures for sharing information within the group for AML/CFT purposes", "at the level of branches and majority-owned subsidiaries in Member States and third countries" (paragraph 1). More particularly, as regards detection and disclosure of suspicions, "information on suspicions that funds are the proceeds of criminal activity or are related to terrorist financing reported to the FIU shall be shared within the group" (also on a cross-border basis).

to be in place to ensure that the FIU that analyses a case reported by an obliged entity established abroad can obtain additional information from this entity (article 53(2), second paragraph).

To complement these innovative forms of cooperation, the Directive assumes that, to properly deal with cases that concern multiple Member States, FIUs need to go beyond the simple exchange of information for the detection and the analysis and share the analytical activity itself; this should be conducted in a joint manner. Traditional forms of cooperation among EU FIUs, though enriched by the innovative instruments recalled previously, are based on facilitating the sharing of information to the benefit of the analytical activities conducted by the FIUs involved. These activities, though, remain confined within each of these FIUs. Under this approach, cross-border cases that involve multiple jurisdictions would be analysed separately by the FIUs concerned. As enriched as these analyses may be, through enhanced forms of exchange and sharing of information, they would still be conducted in isolation and would entail separate assessments (of possibly commonly held information), distinct outputs and possibly diverse follow up.

In this scenario, cases of common interest, subjected to the analysis of multiple FIUs, would trigger ample sharing of information but would still be analyzed separately. Clearly, this approach is sub-optimal as it doesn't fully exploit potential synergies which would derive from a participation of interested FIUs in the evaluation phase, thus limiting the overall effectiveness, and also entail a risk of inconsistency as the same (or closely connected) cases could lead to different assessments and follow up in different Member States without this being possibly justified.

To recall the example mentioned earlier, suspicious cases of a cross-border nature identified and reported by a financial conglomerate through a comprehensive overview at the consolidated group level of operations conducted and information held by units established in different Member States risk being "split" through different FIUs; they would analyse these same cases under their limited national perspectives, ending up with multiple outcomes and possibly differing follow up (which would also result in multiple and potentially inconsistent feedback to the reporting entity as a multinational group).

There is a risk that, while information is amply shared and integrated at the EU level, particularly for the identification of cases of common interest, analyses on these cases based on such common information remain separated at the national level. To limit this risk, the fourth Directive envisages that FIUs should go beyond the sharing of information and, in addition, should be able to perform "joint analyses" on cross-border cases. Article 51 mandates the EU FIUs' Platform with providing advice on the implementation of this innovative activity. At the same time, it is important that EU FIUs have the legal and operational capacity to participate in such joint analyses.

8.2 Legal basis for joint analysis

The majority of EU FIUs have indicated in their responses to the Survey that they can take part in joint analyses, both on a bilateral and on a multilateral basis. Only three respondents have reported that they do not have this capacity, as it is not covered by the applicable domestic legal basis. However, similarly to what has been observed in previous paragraphs in relation to the new information sharing tools introduced by the fourth Directive, responses from those FIUs that have indicated that they can perform analyses jointly highlight that this capacity is based on general domestic provisions empowering the FIU to entertain cooperation with their foreign counterparts, basically through the ordinary exchange of information. In this respect, the responses seem to assume that the same capacity to share information can adequately support also the participation in joint analyses.

The general understanding seems to be that "joint analysis" activities consist in advanced forms of sharing information which naturally evolve in its integrated consideration by the FIUs involved. Under this approach, a view is expressed that the same legal basis underpinning FIUs' exchange of information, also in its new and more advanced forms, should be sufficient to support joint analyses which can be developed based on this information, as a natural consequence and development of such exchange.

A respondent has highlighted that, already in ordinary cooperation among EU FIUs, the number of exchanges significantly exceeds that of requests and responses, so that already now cooperation goes well beyond the mere "request-response" dynamic and results in a much more complex "web" of integrated interactions on cases of common interest.

According to this respondent, in FIU-to-FIU cooperation it is often even difficult to draw clear-cut and precise distinctions between requests and spontaneous disclosures, as well as between replies and feedback; effective cooperation often entails that the requests highlight cases that are relevant also for the requested FIU and thus bring important information that can be evaluated for the requested FIU's own analytical purposes.

Under this perspective, the sharing of cases of common interest and their evaluation, already well beyond simple request-response exchanges, naturally evolves into joint analyses. Thus, the legal basis underpinning FIUs' capacity to exchange information and share cases can also sustain new and more integrated analytical activities.

However, while respondents have confirmed that there are no restrictions explicitly preventing EU FIUs from engaging in joint analysis, it appears that there is equally no explicit authorization or empowerment to cooperate in the conduction of analyses beyond the exchange of information.

8.3 Conditions and limitations to joint analysis

Therefore, it is not surprising in the current picture that several conditions and limitations to EU FIUs' capacity to participate in joint analyses are put forward by many respondents. These conditions and limitations are both specific for this particular activity and generally applicable to all forms of FIU-to-FIU cooperation, in line with what has been highlighted in previous paragraphs.

Some FIUs refer to data protection constraints to which any possible participation in joint analyses would be subject, as well as to the need, in order to engage in such activities, to assess necessity and proportionality of cooperation in light of the cases. Difficulties may increase in engaging in multilateral joint analyses as, in the absence of explicit domestic provisions, forms and extent of cooperation may need to be differentiated having regard to the particular counterparts, due to their different involvement in the cases and availability of information.

Practical obstacles are also identified by respondents, as regards their ability to actively participate in and facilitate joint analyses (by, for example, allowing access to documents, sharing outputs and analytical products, providing clearance to other FIUs' staff to access own premises). Resource constraints are indicated by many FIUs as a significant limitation too. Access to documents may also not be possible in certain cases and the access to FIUs' premises may be subject to declarations of confidentiality.

In addition, all limitations and conditions that generally affect EU FIUs' capacity to provide cooperation would apply also to the participation in joint analyses. Therefore, these would not be possible for a significant number of EU FIUs in the absence of a prior STR/SAR on the same case

subject to the analysis or if investigations or legal proceedings are underway on that case or on the subjects involved. Equally, joint analyses would be impeded for some if a predicate offence is not identified or if it is not criminalized in the same form under domestic legislation. The capacity to engage would also be affected where the case to be analysed jointly is not considered properly substantiated or suspicious and when it relates to tax matters or otherwise involves tax-related information.

Moreover, in cases where participation is possible in joint analysis exercises and these can be started, the constraints that limit EU FIUs' capacity to exchange information (as regards the range of data available or the need for authorizations), already recalled especially in Paragraphs 2 and 3, would equally apply, further limiting the effective implementation of this tool.

One respondent, a police FIU, has indicated that it could not participate in joint analyses with administrative FIUs.

The Survey shows that provisions specifically addressing the performance of joint analyses seem still lacking across EU Member States. Possibly due to the absence of such targeted provisions, important issues are outstanding which seem to considerably limit or condition the capacity of EU FIUs to engage in joint analysis. Against this background, it cannot be said that the Directive has been implemented in this regard.

The views expressed by respondents on their capacity to engage in some forms of joint activities within the existing framework are certainly reassuring about consolidated cooperation practices and can be conducive towards the initial implementation and application of the joint analysis tool. However, it is not clear if the FIUs' capacity to share information and cases, as broad as this may be or become following the proper implementation of the fourth Directive, can support all the activities which can be associated with joint analysis exercises in the absence of dedicated provisions.

In fact, also based on further details that can be set out by the EU FIUs' Platform in accordance with article 51, joint analysis may entail activities beyond the sharing of cases, such as the formation of joint teams of analysts which, through appropriate access to databases of their respective FIUs, conduct common evaluations. These may in turn lead to shared outputs and, although each FIU should of course proceed to dissemination to competent authorities in accordance with its domestic legal framework, coordination for consistent follow up in interested Member States may also be expected.

Ad-hoc and targeted provisions may be necessary for FIUs to be able to safely take part in these activities, also in light of coordination with domestic tasks and possible data protection concerns.

- Appropriate national implementation of course plays an essential role, as FIUs need to rely on domestic provisions allowing them to engage in activities beyond information sharing and removing potential obstacles or conditions (e.g. on data protection or sharing documents and outputs).
- At the same time, common provisions or guidance at the EU level would greatly facilitate this process and limit the risk of inconsistent approaches that may impair the effectiveness of joint analyses.
- Also, in line with the provisions in article 51, the EU FIUs' Platform, valuing recent experiences gained through pilot projects on joint work for the analysis of specific issues, should provide guidance on what this particular cooperation activity entails, beyond the exchange of information, and outline a common "methodology" that could assist FIUs in

future exercises.

8.4 A supranational approach to FIUs' cooperation – Towards a "Financial Intelligence Unit of the EU"

Money laundering and terrorist financing suspicious cases dealt with in STRs/SARs and in FIUs' analysis increasingly have a cross-border nature, in at least two connected respects: potentially illicit activities to be analysed are carried out in, or otherwise involve, multiple jurisdictions; the obliged entities that need to be approached to obtain necessary information and follow the money trail are established or operate in different countries.

As mentioned, conscious that efforts in preventing and detecting money laundering and terrorist financing cannot be confined at the national level, the fourth Directive requires a group-wide approach to AML/CFT compliance by banking and financial groups. This includes the measures and procedures deployed for the identification and reporting of suspicions. To this group-wide approach to compliance with STR/SAR reporting obligations does not correspond, from the FIUs' side, an equally consolidated system for analyzing disclosures or, more generally, suspicious money laundering or terrorist financing cases, that may involve different entities and have a multi-national dimension.

The FIU-to-FIU cooperation in the EU should go beyond the model of FIUs international cooperation which is essentially based on the mere exchange of information on a case-by-case basis, accompanied by certain conditions and safeguards, while the analytical functions continue to remain essentially separated and mostly fragmented along national lines.

The fourth Directive address these weaknesses to some extent and pursue an approach towards a more integrated system for the detection of money laundering or terrorist financing phenomena, the sharing of related information and their effective analysis. This approach is based on a two-pronged strategy: require the sharing of "cross-border" reports, thus addressing some "asymmetries" in the distribution of information on relevant cases across Member States (also due to the particular "territorial" criterion underlying the reporting obligation) that cannot be overcome through ordinary means based on "request-response" exchanges or spontaneous sharing; foster the conduction of "joint analyses" on cases that are of interest of more than one FIU. These innovative mechanisms are extremely important. As emphasised in this Report, they are not yet properly implemented by Member States and should be transposed quickly and effectively

In any event, such mechanisms are affected by some intrinsic limitations and should be considered as intermediate steps of a process that needs to be continued. For example, cross-border reports are only loosely defined in the Directive and, although more targeted criteria may well be developed by the Platform, it may well be the case that reports that will not fall under these criteria (for example, because disclosures are prima facie confined to national contexts) have instead a multi-national dimension (revealed for example through ensuing analysis) and should be shared among interested FIUs for joint consideration and treatment. Also, as regards joint analyses, their inception is entirely left up to individual FIUs: they may have neither sufficient information nor the appropriate incentive to share cases and promote a process of shared analyses together with other counterparts.

As regards the lack of sufficient information, it may be difficult, from the perspective of individual FIUs and based on the information available to them nationally, to appreciate fully when a case or a phenomenon is likely to be of interest to other counterparts to the point that it could be made subject to joint analyses; the identification of the foreign FIUs that may be interested in combining

their efforts may also be difficult, due to possibly uncertain or weak links that, based on the information available, the case feature with particular jurisdictions[175].

As regards the incentive for FIUs, it has to be recalled that the procedures and mechanisms for triggering joint analyses, besides being as yet undefined, may be time and resource consuming. Also due to existing priorities and scarcity of resources, EU FIUs may not even have an incentive to share information spontaneously, let alone carry out joint activities. Moreover, sharing the analytical phase also entails that national FIUs are left with a reduced capacity to "control" the whole process, the related information and the final outcome; they may be dissuaded to engage in such joint activities by concerns of excessive sharing of information, loosing of competences, reduced capacity to provide the national law enforcement agencies with the outcome that they expect. Domestic counterparts, for example those that are the recipients of dissemination or other information from the FIU, which in some cases may also exercise some controls on the FIU and its activities[176] may also have an interest in maintaining the FIU's analysis confined to the national context and may oppose to its joint conduction with foreign counterparts. Existing "confusion" between analysis and law enforcement activities, with related constraints on the former (as also extensively discussed in this Report) and data protection issues can also play a role in limiting the EU FIUs capacity and willingness to foster and promote joint analyses.

Against a background of increasingly interrelated money laundering or terrorist financing phenomena, it is necessary to compensate for these adverse incentives and at the same time bring forward the process of integration of FIUs' activities in detecting, sharing and analysing information on potential money laundering or terrorist financing cases, at the same time ensuring that the requirements of autonomy and independence underpinning FIUs' organization and functions are fully complied with. In addition to devising more advanced forms of FIU-to-FIU cooperation in the current framework which relies on decentralised national operations, a supranational approach to sharing and analysing information should be developed, capable of complementing and supporting activities carried out by FIUs at the national level and current forms of FIU-to-FIU cooperation within the EU.

To pursue such supranational approach, a centralized Financial Intelligence Unit of the European Union ("FIU of the EU") could be set up and entrusted with tasks particularly focusing on the identification of cross-border cases, the consideration of such cases to promote cooperation among national FIUs, the setting up of mechanisms and projects for the conduction of joint analyses. More specifically, an FIU of the EU could perform the following functions:

- facilitate the identification of relevant cross-border cases (based on disclosures from national FIUs but also through the "matching" functionalities of the FIU.NET);
- foster and coordinate the exchange of information between the FIUs involved in the identified cases;
- promote and coordinate joint analyses among European FIUs on cross-border cases that have elements of common interest.

This body could also provide an appropriate response, from the FIUs side, to the group-wide approach to AML/CFT compliance, specifically as regards the reporting obligations for financial

[175] The practice recently developed by the Egmont Group for the multilateral sharing of information for the detection of terrorist financing activities is a good case in point: information is "pushed" to foreign counterparts even in the absence of apparent links with their jurisdictions, precisely because these links are difficult to identify on an ex ante basis, may be known to the receiving FIUs rather than to the sender or may become apparent at a later stage of the analysis.

[176] As discussed in Chapter 2; this may be specifically the case of the bigger organisation where the FIU is located or of police or judicial authorities.

institutions. Subject to appropriate conditions, the FIU of the EU could receive disclosures concerning trans-national suspicious activities, as properly defined. In several instances, reporting to one FIU only (provided this FIU can be identified) or to multiple FIUs would not be efficient and can even create obstacles in terms of duplications, ineffective distribution of information, cooperation. Under a group-wide approach to reporting, suspicions are identified taking account of information coming from multiple branches and different countries and, therefore, are somehow "delocalised"; reporting such suspicions to a particular national FIU, possibly arbitrarily identified, may be difficult and even inefficient.

Moreover, in relation to activities performed by financial institutions operating cross-border by means of agents or on a free provision of services basis the "territoriality" criterion applicable to the reporting obligation may result, as already discussed, in an inappropriate distribution of information among the interested FIUs. These are also cases where a supranational approach based on a coordination role played by an FIU of the EU could ensure that information reach the interested FIUs and that appropriate forms of cooperation are developed among these FIUs, where needed.

Besides coordinating and facilitating national FIUs' analytical and cooperation functions, the FIU of the EU could perform additional tasks in support of FIUs' activities which would benefit from a more uniform approach at the EU level. The following points should be recalled, also in light of previous analysis in this Report.

- The FIU of the EU could identify and share good practices concerning the structure and information content of disclosures related to suspicious cases as well of threshold-based disclosures, also by devising "templates" that could be taken as a reference by EU FIUs to foster their analyses (see the discussion on these points in Chapter 3).

- It could also facilitate common approaches to national FIUs' access to relevant information sources, setting out types of information or databases that fall under the categories of "financial", "administrative" and "law enforcement" and that should be available to EU FIUs as a minimum; this would also address existing differences and shortcomings, as noted earlier.

- The FIU of the EU would also ensure appropriate dialogue and cooperation with other supranational bodies in charge of, for example, law enforcement or supervisory tasks, in a more efficient and effective manner than is now possible for individual EU FIUs.

On this last point, it has to be recalled that the process leading up to broader and more effective forms of FIU-to-FIU cooperation and to the setting up of an EU coordinating body would somehow mirror the development of the EU framework for financial supervision, where the deficiencies arisen in the recent past have been addressed by, i.a., setting up European Supervisory Authorities and creating a Single Supervisory Mechanism entrusted with supervisory actions at the EU level.

Also law enforcement agencies have their coordination mechanisms at the EU level, based on, i.a., the action of Europol and Eurojust. It is not by chance that such investigative coordination encompasses also the AML/CFT law enforcement domain.

The FIU of the EU could therefore effectively liaise with the ESAs and with the European Central Bank, as needed to perform the AML/CFT tasks respectively assigned. Similarly to the relations between FIU's analysis and law enforcement, also the cooperation between FIUs and supervisors is currently confined at the national level thus making it difficult to detect and take due account of

EU-wide AML/CFT issues relevant for supervisory purposes and, on the other hand, of possible suspicious activities detected by EU supervisors which should be considered by FIUs for analysis.

Similarly, the FIU of the EU could cooperate with competent EU law enforcement agencies on matters concerning money laundering and terrorist financing. The EU framework for investigative and law enforcement coordination lacks at the EU level a counterpart on the analytical side, where FIUs operate. As a consequence, cooperation between FIUs and law enforcement agencies only takes place at the national level and the approach to EU-wide cases of money laundering or terrorist financing may not be as effective as it should be.

Finally, as briefly recalled above, it is important that any arrangement in which FIUs' functions, both as regards cooperation and analysis, are attributed to a newly created centralised EU body, is set up under appropriate conditions of autonomy and independence. These conditions should be twofold.

- On one hand, national FIUs should continue to act autonomously and independently from each other and with respect to the EU FIU, while at the same time being bound by enhanced cooperation duties and participating in coordination and information sharing mechanisms. This could be achieved, for example, by ensuring forms of direct participation of national FIUs into the governance and decision-making processes.

- On the other hand, the EU FIU should itself enjoy an adequate status of autonomy and independence, both as regards its resources and the conduction of its functions[177]. More particularly, the EU FIU should remain independent from both national FIUs (which, while collegially participating to the governance, should not unilaterally impose their decisions or refuse to participate in exchanges or joint activities) and from other agencies, at national or EU level. In this latter respect, for example, it would be important to avoid that law enforcement agencies could direct the action of the EU FIU or pull information held or processed by it; similarly, the governance or decision-making procedures should remain rigorously separate from those of any "parent" organization where the EU FIU may possibly be located[178].

9. Obligations for requesting FIUs

9.1 Requirements for the requests

Obligations related to FIU-to-FIU cooperation are not limited to the duties to share ample information; they also include requirements concerning the content that requests should have as a minimum. These requirements are aimed at allowing the requested FIU to have a proper understanding of the case to which the request refers to and of the information needs of the requesting counterpart. Properly motivated requests also allow FIUs to assess the case, in light of the links that it has with their countries, with a view to determining if, in addition to providing the necessary cooperation, a particular follow up is required domestically to identify and analyse possible money laundering or terrorist financing cases or phenomena.

[177] The considerations in Chapter 2 on the implications of the independence requirements for both organizations and functions should be recalled here.
[178] While, at the same time, adequate resources should be made available to the EU FIU for its effective functioning.

The information requirements for requests are set out in article 53(1), second paragraph, of the Directive: "A request shall contain the relevant facts, background information, reasons for the request and how the information sought will be used". As discussed in par. 6, "different exchange mechanisms" can be applied by FIUs, notably based on non-motivated requests and conducted through "Known/Unknown" exchanges carried out on the FIU.NET. All respondents have confirmed that they fully comply with the information requirements stipulated in article 53(1); with the exception of "Known/Unknown" exchanges, requests can be (and are) accompanied by appropriate motivations and explanations.

Respondents also explain that information on facts being analysed are often shared in requests following the particularly ample standards set in this regard by the Egmont Group[179] and that any follow up clarification is always possible in case this is required by the counterpart. In this context, respondents also recall that they include in the requests also the indication of links with the country of the requested FIU and of the way in which the information sought will be used (for example, requesting a consent for domestic dissemination). Requests are also filled in with appropriate identity data allowing, to the extent possible, to identify the subjects involved.

Also, when requests concern particular banking or financial activities, respondents highlight that details of these activities are also included in requests. Details on possible predicate offences, if identified, are also included. Obviously, the information that cannot be shared by EU FIUs due to the existing conditions and limitations (see previous Chapters) are equally excluded from requests.

As already observed, the obligations for the requesting FIUs should not be intended as a condition which, if not properly fulfilled, allows the requested FIU to refuse cooperation[180]. Similarly, the need to describe the case and the grounds for suspicion should not lead the requested FIU to conduct an assessment on the soundness of the request and refuse cooperation when this assessment gives a negative result. In cases of inadequately motivated and substantiated requests a dialogue should be entered into by the involved FIUs to complete the background information and come to a full understanding of the case. At the same time, the requested FIU should provide a preliminary feedback to its counterpart, at least based on the information already available[181]

Based on responses, concerns remain on how far FIUs go in assessing requests and the underlying cases and second-guessing the inherent suspicions to determine if cooperation should be provided and its extent. In any event, information provided by respondents generally show that EU FIUs foster a dialogue in case of incomplete requests and do not simply refuse to provide cooperation.

Clarifications on this point may be beneficial in support of effective FIU-to-FIU cooperation with a view to, at the same time, reinforcing the need for well motivated requests and requiring FIUs to act also on initial requests that need further substantiation. As said previously, in this report, FIUs should not refuse cooperation based on their own re-assessment of the cases at the basis of foreign requests. In this regard, while national implementation is of course of utmost importance in setting appropriate legal bases for FIUs, provisions or guidance at the EU level on how article 53(1), second paragraph, should be interpreted would be beneficial (also, for example, through an opinion or a common understanding issued by the EU FIUs' Platform).

[179] See the Operational Guidance for FIU Activities and the Exchange of Information, n. 19.
[180] In fact, this would amount to a violation to the fundamental obligation to cooperate stipulated under articles 52 and 53(1), first paragraph, of the fourth Directive. See the discussion on this point in paragraph 2.4.
[181] This point also has been previously discussed in paragraph 2.4.

9.2 Use of the information exchanged

Following the responses, the requesting FIU is subject to particular obligations or restrictions concerning the possible use of the information received and applicable modalities. The information provided can in fact only be used "for the accomplishment of the FIU's tasks as laid down in this Directive" (article 54), that is for the analysis (not for investigation) of suspicious money laundering or terrorist financing cases (not of other forms of possible criminality). More broadly, the information exchanged can be "used only for the purposes for which it was sought or provided" (article 55(1)).

Any further use of the information, as well as its dissemination to other authorities is strictly dependent on a "prior consent" by the providing FIU (article 55(1)). In addition to the "purpose limitation" to the use of the information exchanged[182], the transmitting FIU "may impose restrictions and conditions".

All respondents have confirmed that, in conformity with the rule of "purpose limitation", they ensure that the information exchanged is used only for the purposes for which it was sought or provided and is not disseminated or further used without the necessary prior consent of the foreign counterpart. Many respondents highlight that when, based on the prior consent, the received information is further disseminated, this is accompanied by all appropriate caveats (concerning, for example, the use that is possible of the information forwarded), and that all conditions and limitations specified by the transmitting FIU are duly complied with.

Respondents emphasize that any authorized dissemination of the information received from other EU FIUs is carried out with all appropriate safeguards to ensure that the subsequent use (normally only possible "for intelligence purposes") strictly adheres to any limitation or condition related to, for example, the purposes and the subjects that can be involved. Confidentiality and security measures are also implemented by FIUs to ensure that no improper use occur of the information received[183].

Respondents also indicate that they apply practical measures to ensure appropriate protection of disseminated information and compliance with possible restrictions specified by the counterpart FIUs together with the necessary consent.

- The foreign providing FIU may not be mentioned, unless this indication is needed for domestic recipient agencies to file MLA requests to competent authorities of the country involved.
- The information may be forwarded in a sanitized format, that is without references to the communication received from the foreign counterpart or details on it.
- Also, it can be explicitly indicated that the transmitted information should be protected and kept confidential and that it is not to be used for evidentiary purposes in court proceedings and can only be further shared subject to an ad-hoc consent by the originating FIU.

Responses to the Survey refer to the implementation, through appropriate instructions, of handling conditions or clearance restrictions to the FIU's staff, aimed at ensuring that received information is not used or processed beyond what is allowed under the general "purpose limitation" principle or in accordance with any possible specific instructions provided by the transmitting counterpart. The dissemination is also normally only disposed based on managerial decisions and is not left to the initiative of individual employees.

[182] The purpose limitation and its implications have been discussed in par. 1
[183] See also Chapter 8 on the confidentiality regime applied.

However, some respondents note that, when they provide a consent for further use or dissemination of the information transmitted, together with caveats and conditions, they often realize that this information is treated or disseminated beyond the scope of the authorization. On the other hand, respondents also note that often times, after disseminating the information received from foreign FIUs following the prior consent and based on its terms, they lose the control on the information itself and on how it is further used or disseminated. It is observed that it is not possible for the disseminating FIU, despite the scrupulous adherence to all conditions set by the foreign counterpart and any best effort deployed, to monitor the subsequent use of the information along the domestic "dissemination chain", to make sure that this complies with the terms of the consent and with any associated conditions. These difficulties are particularly relevant when the dissemination is done towards prosecutors[184].

On this particular aspect, one respondent specifies that, while all caveats are always duly recalled in the authorized dissemination about the allowed use of the information and appropriate safeguards are applied, it is inherent to dissemination that the actual control on how the information will be used and protected by domestic recipient parties is "loosened". The same respondent refers to instances where, despite all safeguards and caveats by the FIU, the information has been used or divulged contrary to, or beyond, what was allowed by the providing foreign FIU.

This is most often the case of information which, based on criminal procedure laws, passes from the intelligence or investigation to the judicial phase and is therefore used in the context of legal proceedings. This respondent additionally notes that, while the control that can be exercised by the FIU in these cases on how the information is used is very limited, domestic criminal procedure laws may prevail on provisions on FIUs' cooperation; as a consequence, the purpose limitation and the constraints associated with the (lack of) consent may be overruled.

10. Consent for further use or dissemination of the information exchanged

10.1 Limits to the use and dissemination of the information exchanged. The prior consent

Based on the purpose limitation rule, information exchanged among FIUs can only be used by the receiving FIUs themselves, with no further dissemination to other parties (domestic or foreign) or other forms of divulgation. Moreover, the information can only be used in support of the analysis function of that FIU, not for other purposes such as for investigation or as evidence in criminal proceedings[185] or for supervisory purposes. Also, the exchanged information can only be used for pursuing (through analysis) suspicious money laundering (and its predicate crimes, insofar as they are "associated" with the ensuing money laundering) or terrorist financing cases, not other forms of potential criminality[186]. In addition to the general restrictions associated with the purpose limitation,

[184] More on this in par. 10.9.

[185] This may be particularly important in case of police or judicial FIUs.

[186] See article 54 of the Directive: "Information and documents received pursuant to Articles 52 and 53 shall be used for the accomplishment of the FIU's tasks as laid down in this Directive". Also, under article 55(1) "Member States shall ensure that the information exchanged pursuant to Articles 52 and 53 is used only for the purpose for which it was sought or provided and that any dissemination of that information by the receiving FIU to any other authority, agency or department, or any use of this information for purposes beyond those originally approved, is made subject to the prior consent by the FIU providing the information".

as discussed previously, the receiving FIUs must abide by any conditions or limitations set out by the FIU providing the information on how such information should be used[187].

These limitations to the use of the information exchanged can be overcome through a specific "consent" granted by the FIU from which the information originates. To reinforce the prohibition to use the information beyond the established purposes in the absence of such consent, the Directive (in line with the FATF and Egmont standards) clarifies that it has to be "prior" to the intended further use or dissemination. The providing FIU must be informed and requested in advance about the intended use or dissemination and these only become possible when the consent is confirmed.

Therefore, due to the limitations recalled above, the information exchanged, while fully usable for the internal analysis performed by the receiving FIU, cannot accompany the output of this analysis through the ensuing dissemination to competent law enforcement bodies in charge of investigating or prosecuting the potential money laundering or terrorist financing cases (unless prior consent is given). This constraint is applicable despite the dissemination being an essential core function of FIUs which naturally follows analysis and aims at ensuring that its results are put to good use. In the absence of an ad-hoc consent, information received from a foreign FIU cannot be forwarded through dissemination even if the analysis has highlighted a well-founded money laundering or terrorist financing case precisely based on the information obtained through international cooperation.

In fact, like analysis, dissemination is a core function of FIUs, in light of their very definition (see article 32(3) of the Directive). More precisely, analysis is not carried out as an isolated task and for its own sake but is specifically aimed at gathering information and extracting intelligence intended to support subsequent action by competent bodies. This finality, inherent to FIUs' core activities, can only be achieved if relevant information and intelligence, as resulting from the analytical process, is forwarded to those competent bodies, precisely by means of dissemination[188]. It can be said that an FIU can only achieve the purpose it is intended to serve if it is able to disseminate the intelligence produced. Good analysis is instrumental to support and add value to investigations and would be useless if its results and the related information could not be forwarded to competent agencies for appropriate follow up. Insofar an FIU manages to operate effectively in support of investigations and prosecutions as it manages to disseminate intelligence and relevant information[189]. In other words, the more the FIU disseminates, the more it effectively contributes to detecting and countering money laundering and terrorist financing, provided that quality analysis is performed.

While, in pursuance of its fundamental functions, all information used in, or obtained from, the analysis can be disseminated, to the extent of course that this is relevant to add value to ensuing investigations, this does not apply to information obtained from foreign FIUs (either spontaneously or on request, either through cross-border disclosures or in any other form allowed by international exchange mechanisms). As said, in fact, this information can only be disseminated if a prior consent

[187] According to article 54, "When exchanging information and documents pursuant to Articles 52 and 53, the transmitting FIU may impose restrictions and conditions for the use of that information. The receiving FIU shall comply with those restrictions and conditions".

[188] Of course, reference here is made to the so called "spontaneous" dissemination, that is the action of forwarding information deriving from analysis that FIUs perform upon their own initiative and based on appropriate selection of cases and information: see article 32(3) of the Directive. Dissemination "on request" from domestic law enforcement bodies, foreseen by article 32(4) of the Directive, is not necessarily based on ad-hoc analyses and is simply a form of sharing of STR information that EU FIUs are called on to carry out (in line with international standards and subject to certain conditions) following specific requests. See also Chapter 5 on these aspects.

[189] Provided also that adequate selection is ensured, allowing competent investigating bodies to focus on relevant cases and information: see Chapter 5 on the features of analysis and dissemination.

is granted by the providing FIU. The dissemination function, and therefore the overall effectiveness of the FIU's action, is dependent, in this respect, on counterparts' authorizations. This condition becomes particularly important when the information obtained from foreign counterparts is key to qualify the case as related to money laundering or terrorist financing and to pursue it through effective investigation.

Hence, the importance of the prior consent as a crucial element both for effective domestic analysis and for international cooperation: exchanging information to develop good analysis, even to the broadest extent possible, is useless if this information cannot be disseminated, when needed, due to the absence of the required consent. The more the consent is denied, the more FIUs' cooperation is frustrated and becomes ineffective, together with the associated analysis.

It is not by chance that, in fact, the Directive makes it an obligation for FIUs to provide the consent for further use or dissemination, when requested by EU counterparts. More precisely, article 55(2) establishes that "Member States shall ensure that the requested FIU's prior consent to disseminate the information to competent authorities is granted promptly and to the largest extent possible".

However, this obligation is not unconditional as the consent is only due "to the largest extent possible". The Directive itself explicitly envisages instances where FIUs can legitimately refuse their consent. These circumstances are described in broad terms: according to article 55(2), "The requested FIU shall not refuse its consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the Member State of the requested FIU, or would otherwise not be in accordance with fundamental principles of national law of that Member State". This provision leaves Member States and FIUs with a particularly wide room for implementation and interpretation in determining cases where the consent can (or should) be denied.

As will be described in more details in the following paragraphs, the responses show that this results in ample discretion in deciding upon the consent and in an equally ample scope for exceptions, to the detriment of effective FIUs' cooperation through the appropriate use of the information exchanged. Limitations in granting the consent, as said, have repercussions on the FIUs' dissemination function, particularly as regards the completeness of the information that can passed on to competent law enforcement agencies to effectively pursue money laundering or terrorist financing cases.

The following paragraphs are dedicated to an overview, and a related analysis, of existing conditions and limitations that prevent EU FIUs from providing their consent for the use or dissemination of the information exchanged to a sufficiently broad extent, falling short of the requirement in the Directive to grant such consent "to the largest extent possible"[190]. Paragraph 10.2 highlights how, due to the particularly large and undefined scope of the derogations allowed by the Directive, the general duty to grant the consent is subject to discretion and be exercised on an exceptional basis rather than as a rule. Subsequent paragraphs 10.3 to 10.8 then describe and discuss the limitations to the consent, as highlighted in the responses to the Survey and against the background of the derogations foreseen by the Directive.

Finally, paragraphs 10.9 (10.9.1 to 10.9.3) elaborate on conclusions and proposals on how the scope of the duty to consent should be clarified and broadened, by properly reinforcing the EU provisions

[190] The extent "possible" under national laws does not appear broad enough to allow that information obtained through FIU-to-FIU cooperation can be properly used through effective domestic dissemination.

in this regard and allowing that the information exchanged through FIU-to-FIU cooperation can be effectively used in investigations or legal proceedings (facilitating MLA initiatives, when appropriate, and without interfering with law enforcement or judicial cooperation mechanisms).

10.2 Capacity to provide the consent. General scope, limitations and conditions

EU FIUs confirm in their responses to the Survey that they are able to grant the prior consent to further use or dissemination of the information provided promptly and to the largest extent possible, as required by article 55 of the Directive[191].

This capacity, however, seems to encounter considerable limitations due to a range of conditions applicable in several Member States. FIUs are in fact often prevented from consenting to further use or dissemination or are bound by particular restrictions. Moreover, ample room is left for discretion, as it appears that in many cases FIUs, under national law, are only allowed to provide the consent, rather than required to do so. Also, significant discrepancies exist among national regimes applicable to EU FIUs as far as their capacity to provide the consent is concerned.

The responses received seem also to indicate that the consent, rather than a straightforward obligation, is often dependent on discretional decisions, which are taken on a case-by-case basis by the requested FIU in light of a number of circumstances, and only rarely or partially stem from objective criteria.

Responses also suggest that, in some cases, the scope of exceptions may be broader than the area of cases where the FIU is required, or even simply empowered/allowed, to grant the consent. Given these circumstances, the consent may be the exception rather than the rule.

On the other hand, the considerable room left to national implementation also translates into significant differences among EU FIUs as to the cases and conditions under which the prior consent can be granted or refused. These discrepancies not only add on to the difficulties of FIUs' cooperation stemming from the need to take account of different regimes for the consent applicable to FIUs engaged in exchanges; they also play an indirect, but more general, adverse role on cooperation via the reciprocity principle. In fact, as discussed for previous similar cases, FIUs with a lower capacity to grant the consent may trigger reciprocity "retaliations" by pushing other FIUs to apply the same restrictions which, although not foreseen by their national law, become equally due because of the lack of reciprocity.

Importantly, the conditions and limitations which apply in general to FIUs' cooperation (see paragraphs 1 and 2) refer also to the matter of providing the consent for further use of the information shared beyond the original purpose, especially in the context of investigations or prosecutions. Moreover, the capacity to provide the prior consent is affected by special limitations specifically allowed by the Directive (article 55(2)) and extensively reflected in national legislations. Due to the overly general language that the Directive adopts in crafting these exceptions and to their broad scope, respondents have not been able to specify precisely how these translate into particular national provisions concerning instances where the consent can (or must) be refused.

[191] One respondent, however, has explicitly indicated that it cannot grant the consent in accordance with the conditions established in the Directive.

10.3 The requested use or dissemination "falls beyond the scope of application of domestic AML/CFT provisions"

The vast majority of EU FIUs have confirmed that they are bound by limitations in granting the consent when this goes beyond national AML/CFT provisions. Only 4 respondents are not subject to these constraints. 13 EU FIUs are required to perform case-by-case evaluations to determine if the consent should be refused under this derogation clause, due to applicable conditions and limitations in their domestic laws. For 9 FIUs an outright prohibition is in place to give the consent in such cases.

It is not clear what "domestic AML/CFT provisions" are specifically referred to by the Directive and, therefore, if refusals to grant the prior consent are allowed with respect to any such provision. In principle, all the AML/CFT provisions implementing the Directive may fall into this scope, including on matters such as customer due diligence, record keeping, or suspicious transactions reporting. An alternative, more focused interpretation would target only those provisions which specifically concern the offences of money laundering and terrorist financing or applicable to investigations or prosecutions related to these crimes.

Several responses seem to indicate that this latter, narrower, interpretation has been mostly followed by Member States. In general, derogation clauses allow or compel FIUs to refuse the consent if the information exchanged is to be used for pursuing crimes that are not provided for as such in the country of the requested FIU; or if the sanctions foreseen in the requesting jurisdictions for the crimes that are being pursued would be considered as disproportionate or against human rights.

Clearly, in cases where the consent depends on the type of the underlying criminality the requesting FIUs is expected to provide all necessary elements demonstrating that a crime may indeed have taken place and what type of offence is at stake.

As already recalled in par. 2.3 in relation to the analogous requirement applicable at the phase of the initial exchange of information, this indication about the possible underlying criminality may not be available to the requesting FIU. This, in fact, may only have available the intelligence deriving from the analysis developed that far (that is, until the request for consent is filed). Specific types of crime may not be identifiable on this basis only. The threshold consisting in the description of such crimes can therefore prove inappropriate or excessively high to allow for meaningful FIU-to-FIU cooperation in the dissemination phase. For these reasons, cooperation may encounter significant limitations in these instances.

It has to be added that "dual criminality" conditions are not specifically envisaged by the Directive at the FIUs' level of cooperation. As said, article 55(2) generically refers to cases that "fall beyond the scope of application" of domestic provisions and it may not be clear whether differences in the criminalization of predicate crimes safely falls into this scope. The Directive does not deal, in fact, with law enforcement or criminal law matters, where the "dual criminality" requirement typically lies. This constraint is indeed normally only applicable to police and judicial cooperation mechanisms which, in fact, are geared toward the identification of evidence to be used in legal proceedings for purposes of, i.a., criminal conviction, seizure or confiscation. It would not seem appropriate to anticipate these concerns, and the evaluation of criminal aspects associated with the type of predicate offences, at the intelligence and analysis stage where FIUs' cooperation lies.

Despite these considerations, the majority of EU FIUs are prevented from providing their prior consent for the use or dissemination of shared information, or are subject to particular conditions or

limitations in providing this consent, due to the type and nature of the alleged underlying offences, specifically depending on whether or not they are also criminalized in their domestic legislation.

5 EU FIUs have indicated that they are prevented from providing their consent in circumstances where the "dual criminality" condition is not fulfilled, that is when a particular type of criminality is not identified or, when indicated, it is not criminalized domestically in the same form. 10 FIUs have reported that in such cases, although providing the consent is not prohibited, its provision is nonetheless subject to conditions or limitations.

Also, the FIUs that have responded that the consent can in principle be granted in cases where the potential underlying criminality is not indicated or is different have informed that limitations and conditions can however be attached to this consent concerning the use that is possible of the information exchanged. These conditions and limitations are mostly related to the need to confine such use to only pursuing "intelligence purposes". This normally includes intelligence developed, beyond the analysis performed by the FIU, through investigations carried out by law enforcement agencies but certainly (and often times explicitly) leave out any use by judicial authorities in the context of legal proceedings.

10.4 Existence of criminal investigations or legal proceedings in the country of the requested FIU

Besides the limitations deriving from the scope of domestic AML/CFT provisions, as far as the existence and the type of the criminality pursued in the country of the requesting FIU is concerned, FIUs are often also prevented from providing the prior consent in cases where criminal investigations or legal proceedings are ongoing on the same or related cases in their countries. This limitation is different from the "dual criminality" requirement discussed in the previous paragraph and applies in addition to it.

14 respondents have indicated that, in cases where investigations or legal proceedings are underway in their countries, they cannot freely authorize foreign counterparts to further use or disseminate the information provided. Like similar restrictions that, as recalled, apply at the previous stage of the exchange of information[192], respondents have clarified that the consent in these cases may be conditioned to authorizations released by law enforcement agencies or competent prosecutors that have to be approached for this purpose. Respondents, mostly, have highlighted that these authorizations are decided upon on a case-by-case basis and are largely discretional, depending on whether or not the authorizing authority believes that the ongoing investigations or prosecution might be jeopardized[193] or that the police or judicial cooperation channels should rather be used, instead of the FIUs' cooperation channels, to allow the information to be passed on to investigating bodies in the country of the requesting FIU.

A respondent has reported that it cannot grant the consent due to the mere existence in their countries of investigations or prosecutions, regardless of any possible authorization by a third party (such as competent law enforcement or prosecutorial bodies).

As already recalled, (see, for example, par. 2.2), limitations and conditions to FIUs' cooperation associated with the existence of investigations or legal proceedings are not in line with the provisions in the Directive. The mere existence of investigations or prosecutions is not envisaged as a valid ground for refusing to provide cooperation, neither at the initial stage of the exchange of

[192] See paragraph 2.2.
[193] So it appears that these cases essentially overlap with those considered later, in the next paragraph.

information nor when it comes to consenting the further use or dissemination of such information.

In light of the responses received, however, FIUs' cooperation seems considerably limited, in relation to the capacity to grant the consent, because of the mere existence of investigations or prosecutions in the country of the requested FIU. The extent of these undue derogations to the fourth Directive, therefore, appears particularly broad with potentially significant implications on the FIUs' capacity to provide inputs to domestic investigations on money laundering and terrorist financing cases through the dissemination of information received from foreign counterparts.

10.5 Impairment of a criminal investigation

Differently from the instances described in the previous paragraph, concerning refusals or limitations to the prior consent due to the simple existence of an investigation or a legal proceeding in the Country of the requested FIU, based on the provisions in the Directive such refusals or limitations are allowed in cases where existing investigations or criminal proceedings may be impaired by the requested use or dissemination of the information exchanged.

This conclusion follows directly from article 55(2) which, as recalled above, allows FIUs to refuse their consent to dissemination when, i.a., this "could lead to impairment of a criminal investigation". The same derogation is expressed in the Council Decision 2000/642/JHA (see article 5(3) (which refers to article 4(3))[194]; it also finds a precise correspondence in the FATF standards[195].

The vast majority of respondents have in fact indicated that the consent cannot be provided, or is subject to conditions or limitations, when the requested use or dissemination is likely to cause the impairment of domestic ongoing investigations. The conditions and limitations that respondents are subject to are mostly related to the need to obtain ad-hoc authorizations by a competent law enforcement agency or a prosecuting magistrate (see also the considerations in the previous paragraph on this point).

Although responses to the Survey have not flagged this concern specifically, FIUs may not be aware of criminal investigations ongoing in their jurisdictions on cases or subjects involved in a request for assistance received from a foreign FIU. Even in cases where they happen to know that relevant investigations are underway, FIUs may not be in a position to determine whether granting the consent to a foreign counterpart to further use or disseminate the information exchanged is likely to impair such investigations. Because of this, there is a risk that, any time that the FIU is aware of ongoing investigations it simply refrains from providing the consent, using its discretion to avoid any possible risk of impairment[196].

While these issues may arise more acutely for administrative FIUs that do not have appropriate information sharing and coordination arrangements in place with their domestic law enforcement counterparts, suitable mechanisms should be established at the national level to allow the FIU to

[194] Under the Decision, in fact, "an FIU may refuse to divulge information which could lead to impairment of a criminal investigation being conducted in the requested Member State".

[195] The FATF Interpretive Note to Recommendation 40 is even more explicit in stating that FIU-to-FIU cooperation should not be limited by the mere existence of investigations or legal proceedings and can only be refused in cases where the assistance could impede investigations or legal proceedings in the country of the requested FIU (see also the following par. 10.9.2.

[196] As previously discussed, these issues are sometimes addressed in Member States by simply making the FIU's capacity to exchange information or to provide the consent subject to a prior authorization by competent prosecutors; this of course goes to the detriment of both the effectiveness of the cooperation and the FIU's operational independence.

become aware of investigations possibly linked with international exchanges and evaluate if granting a consent could jeopardise such investigations. In any event, the FIU (and its staff) should be protected from any possible undue responsibility; it should also be clear that the decision to grant the consent is taken by the FIU based on the information it has available, or can obtain through appropriate means, on whether relevant criminal investigations exist in its jurisdiction and on the risk that of impairing them.

As also discussed later in par. 10.9.2, clarifications on these points could be provided through EU provisions, so as to allow unequivocal and uniform national implementation.

10.6 Disproportion with legitimate interests and contrast with fundamental principles of national law

The fourth Directive, as mentioned, allows FIUs to refuse to provide their prior consent when the requested use or dissemination would be disproportionate with respect to "legitimate interests" of natural or legal persons or would be against "fundamental principles" of domestic law. As in other areas, the provisions on this point in article 52(2) of the Directive are quite general, leaving the interpretation of the notions of "legitimate interest" and "fundamental principle" entirely open to Member States and to FIUs. This is reflected in a particularly broad scope of application of these general clauses in national legal frameworks and on a considerably diversified understanding of instances that would fall into this scope across different countries and FIUs.

Only few respondents have indicated that they can provide the prior consent without a need to assess whether this could affect legitimate interests of individuals potentially involved (5 FIUs) or infringe fundamental legal principles (3 FIUs). The vast majority of EU FIUs are allowed or compelled to refuse the consent under the circumstances at stake, which they are responsible to assess under their domestic legislations. However, responses vary considerably for what concerns the description of cases which fall under either the "legitimate interest" or the "fundamental principle" exceptions.

In general, it seems that domestic laws applicable to FIUs' cooperation do not define these notions, thus leaving FIUs with a particularly broad room for implementation. Some cases are reported by respondents which could fall under this scope. Examples mentioned in the responses refer to the existence, in the country of the requested FIU, of forms of punishment for the pursued crimes which are in contrast with the protection of human rights, such as death penalty or other forms of inhuman treatment (this could qualify as a violation of fundamental principles of domestic laws). Also mentioned are cases where the rule of law is not considered to be adequately enforced in the Country of the requested FIU, which is considered a fundamental principle, as well as cases where criminal proceedings may be particularly lengthy, which may raise concerns of disproportion with respect to individuals' legitimate interests.

In the absence of targeted definitions, either in the Directive or in domestic laws, several respondents seem also to be of the view that cases where the offences which would be pursued in the country of the requesting FIU are different or not criminalized under the domestic legislation would also trigger derogations to the prior consent, on grounds of either the violation of fundamental principles (namely, the dual criminality principle) or of the disproportionate treatment of individuals' legitimate interests[197].

[197] See, on this point, previous considerations in various paragraphs in this Chapter on the limitations to FIUs' cooperation stemming from concerns about the existence and nature of possible underlying crimes.

10.7 Tax-related cases or information

Responses to the Survey show that significant limitations to the FIUs' capacity to grant the prior consent continue to exist when the case or the requested further use or dissemination may relate to tax matters or involve tax information[198].

Two respondents have confirmed that they are prohibited from providing the consent in such cases. Others have indicated that the consent can only be granted if the case does not relate to tax matters solely but involves other associated predicate offences such as frauds, forged documents, false bank statements.

Other responses have highlighted that, while tax information cannot be provided and therefore its use cannot be authorized, in cases where no tax information is involved the consent for further use or dissemination can be given, regardless of whether or not a tax offence is being pursued as a predicate crime for money laundering. In these latter instances, therefore, the limitations seem to be focused on the type of information and not on its use: tax information cannot be made available but the authorization for the use of the information exchanged for tax-related money laundering cases can be given.

It is important to recall, on this point, that article 57 of the Directive stipulates that "differences between national law definitions of tax crimes shall not impede the ability of FIUs to exchange information or provide assistance to another FIU". While the "prior consent" element certainly falls into the scope of the general obligation to "provide assistance" (which goes beyond the exchange of information, mentioned separately), it does not seem that this provision in article 57 can be read as entailing a straightforward prohibition to refuse cooperation through consent for pursuing tax-related money laundering cases. The more so, as the same article specifies that this provision is not unconditional but is applied only "to the greatest extent possible under national law", thus leaving ample room for exceptions or derogations[199].

This seems to entail that national provisions can well provide, at least to a certain extent, for limitations to the duty to provide cooperation (either through the initial exchange or the subsequent consent) in tax-related matters. Given that tax offences are recurring predicate crimes in significant money laundering cases across EU Member States, the "fiscal excuse" should not be allowed as a derogation to FIUs' cooperation obligations.

To remedy these shortcomings, which certainly unduly limit the capacity of EU FIUs to exchange and use information in such an important area, a proper strengthening of the EU legislation seems highly advisable. The FATF standards should be recalled on this point: the Interpretive Note to Recommendation 40 explicitly prohibits refusals to provide assistance "on the grounds that (…) the request is also considered to involve fiscal matters".

10.8 Other conditions

Similarly to what happens at the prior stage of the exchange of information, several respondents have indicated that the consent for further use or dissemination requires that the case and the

[198] As discussed in par. 2.3, FIUs are sometimes prevented from exchanging information in the first place, when tax issues may be involved. In these cases, of course, where the information is not even made available to the requesting FIU, the issue of the further use or dissemination does not even arise.

[199] Also the general obligation for FIUs to provide their prior consent under article 55 of the Directive (applicable also in tax-related cases) does not seem an absolute one since, as already discussed, FIUs are required to give this consent "to the largest extent possible".

request be properly substantiated and motivated, particularly as regards the grounds for the suspicion. The consent may be refused if the case to which the request refers is not considered relevant or suspicious. For many of these respondents, this requirement goes together, and applies jointly, with the need to specify the underlying predicate offences.

The considerations developed in par. 2.4 on the risks associated with a re-assessment of the case by the requested FIU, which could second-guess its relevance rather than recognizing, and relying on, the judgment of the requesting counterpart, should be recalled here, together with the concerns about potential undue limitations on FIUs' cooperation. The more so, as responses on this point seem to indicate that requests for consent, and their soundness and adequacy, are mostly evaluated by FIUs on a case-by-case basis in a framework of ample discretion.

In some instances, consent to the use or dissemination of the information exchanged cannot be provided if the same case to which the request refers has not been reported also to the requested FIU domestically as "unusual" and if the analysis performed by this FIU has not determined that the case is indeed a proper suspicious one which, as such, should be disseminated to domestic competent law enforcement authorities. These are situations where it appears that the requested FIU can consent to dissemination by the foreign FIU only if the same information is also disseminated domestically (in the event that the related analysis gives a positive outcome), despite the two national contexts being potentially different and of the existence of a substantiated suspicion identified in the country of the requesting FIU where, therefore, the information exchanged can be useful in support of possible investigations or prosecutions.

This seems to amount to an undue limitation to the FIU's capacity to provide the consent, difficult to root into, or even to reconcile with, the grounds for derogations specifically allowed in article 55(2) of the Directive. It is a shortcoming with should be adequately addressed through better domestic implementation of EU provisions in this matter.

On a positive note, responses indicate that the consideration of the status of the requesting EU FIU does not play any role in the decision to grant the consent. This can be given, if other conditions are fulfilled, regardless of the nature of the counterpart and, more specifically, even if this is different from that of the requested FIU.

10.9 Conclusions and proposals

Based on the overview and analysis conducted in previous paragraphs, the EU FIUs' capacity to provide the consent to foreign counterparts to disseminate their information for use in criminal investigations or proceedings[200] (or, more broadly, to disseminate their information to law enforcement bodies or prosecutors) is significantly impaired especially in two circumstances:

- when the predicate crime is not identified in the request or not criminalized in the Country of the requested FIU or, in some cases, when it is a tax offence (conditions of "double criminality" and "fiscal excuse");

- when, regardless of the type and nature of the possible underlying criminality, there are investigations or legal proceedings underway on the same cases in the country of the requested FIU.

[200] Similarly to domestic information obtained through, for example, STRs or related analyses and disseminated to competent authorities for investigation or prosecution.

These are typically conditions that apply in the context of Mutual Legal Assistance forms of cooperation, which aim at the identification of evidence to be used in decisions taken by law enforcement agencies, prosecutors or courts on matters concerning, for example, seizure, confiscation, conviction. In that different context, concerns about the type of crimes pursued and the potential impacts on existing law enforcement activities are certainly well placed and can be tackled effectively by the agencies involved, based on a proper assessment of all investigative elements available to them.

Anticipating these concerns and considerations at the prior stage of FIUs' cooperation, even though in relation to the phase of the consent for further use or dissemination, appears at the same time incongruous and counterproductive. As a way to recap the main arguments developed in this Chapter, the following considerations can be put forward on these aspects in particular.

- FIUs deal with the analysis of suspicious facts. Differently from law enforcement agencies that are involved in the investigation of specific offences, FIUs are not normally in a position to assess if crimes are being or have been committed and, even more, what is their type or nature.

- Requiring FIUs to assess the possible underlying criminality, based on their analysis functions, and making the consent (and the dissemination that depends on it) subject to this assessment deprives law enforcement bodies and prosecutors in the Country of the requesting FIU of relevant information[201], to the detriment of the effectiveness of the FIUs' dissemination for pursuing crimes and, in turn, of the capacity of competent agencies to develop investigations and prosecutions[202].

- Subjecting FIUs' dissemination of foreign information to considerations on underlying offences (based on dual criminality conditions) and ongoing investigations duplicates the requirements and conditions which apply at the ensuing stage of police and judicial international cooperation, where these elements can be more adequately considered.

10.9.2 Re-casting cases of derogation to the consent

To address the problems identified in FIU-to-FIU cooperation, based on the responses received and the analyses conducted in previous paragraphs, the following measures and initiatives can be put forward for consideration.

The general provisions in article 55(2) of the fourth Directive about cases where the consent can be refused, crafted and phrased in overly general terms, should be better detailed and specified. These cases should be reasonably narrowed down, so as not to overturn the general obligation to provide the consent to the largest extent possible, also set out in article 55(2). Mostly, cases for refusing or limiting the consent should be confined to the instances described in the following points.

- An ongoing investigation could be seriously impaired in the country of the requested FIU should the information exchanged be used as requested by the FIU applying for the prior

[201] It has to be noted again that, different from foreign information, domestic STRs/SARs and analytical outputs are routinely forwarded by FIUs to law enforcement agencies and prosecutors in discharging the essential dissemination function.

[202] These, of course, would remain fully subject to all applicable MLA procedures and attached conditionalities in cases where police cooperation channels need to be activated.

consent[203]. Appropriate mechanisms should be in place whereby the FIU is informed about relevant criminal investigations and the risk of impairment deriving from granting the consent.

It is important to underscore that the FATF Interpretive Note to Recommendation 40 is particularly explicit in limiting the scope of possible refusals to international cooperation to cases where "the assistance would impede an inquiry, investigation or proceeding", at the same time specifying that requests for assistance should not be refused on the sole ground that an inquiry, an investigation or a proceeding is underway in the country of the requested authority[204].

- The information is to be used by prosecutors or judicial authorities as evidence in the context of legal proceedings. In these cases, however, whilst limitations to the use of FIUs' information for judicial purposes seem reasonable[205], the dissemination per se should nonetheless be possible.

This last point appears particularly important and is illustrated in more details in the following paragraph.

10.9.3 Consenting the dissemination to law enforcement agencies and prosecutors, not the use as evidence

It is the use of the information for evidentiary purpose that could be refused by the providing FIU on the ground that this use should be made subject to the activation of the appropriate MLA mechanisms and to the conditions applicable in this context (including about possible dual criminality requirements). The dissemination of the information exchanged between FIUs should in any case be possible (and thus authorised through the consent) precisely with the aim to allow competent law enforcement agencies or prosecutors to trigger MLA requests for the use of that information for evidentiary purposes.

Under this approach, the dissemination should be consented, similarly to what has been described above in relation to the use for purposes of further intelligence. In fact, making the information available to law enforcement or prosecutors conducting a legal proceeding would be instrumental to allowing these bodies to consider undertaking MLA initiatives, to which the use of the information as evidence (that is, beyond the mere "intelligence purpose") would still remain subject. Consistently, the consent for the dissemination would be given by FIUs in such cases under the condition that the information will be used solely for MLA purposes and is not be used directly as evidentiary material in the context of the ongoing legal proceeding.

---

[203] This would be in conformity with articles 4(3) and 5(3) of Decision 2000/642/JHA and with FATF stamdards,, as previously mentioned.

[204] This would amount to what the Interpretive Note to Recommendation 40(2)(c) labels as a "unduly restrictive measure": "Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that (…) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding".
This FATF standard provides a good basis for reinforcing the EU provisions on FIUs' capacity to exchange information and grant the consent to use it.

[205] In fact, while FIUs' information should normally be used for intelligence purposes in the context of investigations, the exchange of evidentiary material should be carried out by means of ad-hoc police or judicial cooperation mechanisms and channels.

On the other hand, the FIUs' consent to such dissemination for mere information purposes should not be conditioned to the identification of a predicate offence and to the criminalization of this offence in the country of the requested FIU. As a consequence, FIU-to-FIU cooperation would not be unduly affected by "dual criminality" concerns which would be more adequately dealt with in the subsequent MLA stage by competent law enforcement or judicial authorities.

Under such an approach, therefore, the limitations applicable to the provisions of the consent by FIUs would be referred not to the dissemination to particular recipients but to particular uses of the information exchanged, in keeping with the rules applicable to MLA mechanisms. The providing FIU would still retain control on its information, as any use of that information as evidence would continue to be limited or inhibited, but would not unduly limit its cooperation.

By allowing dissemination of FIUs' information to law enforcement or judicial bodies, regardless of the indication and evaluation of the type of possible crimes involved, these bodies would be put in a position to assess its relevance and, when appropriate, file proper MLA requests for using that information in particular legal proceedings. Only at this stage, in accordance with the legal regime applicable to police and judicial cooperation, the indication of the crime and its type becomes relevant and should be included in the request.

This approach would thus ensure that FIU-to-FIU cooperation, devoted to analysis of suspicious transactions (and to the inherent dissemination), is not obstructed at the dissemination phase and is not frustrated in its basic purpose, which is precisely to provide support to ensuing investigations and prosecutions by adding value through intelligence based also on meaningful foreign information. At the same time, all evaluations on the possible use of the information for evidentiary purposes would be in no way prejudged in the subsequent stage of police or judicial cooperation, which would always have to be triggered for this purpose. In this context, as said, all relevant considerations on the type of the predicate offence and the terms of its criminalization, including in accordance to the "dual criminality" requirement, would remain entirely possible.

This approach may however encounter some practical difficulties which need to be carefully considered and tackled through appropriate measures. These should be preferably taken at the EU level to ensure adequate levels of uniformity and confidence across Member States and competent authorities.

These difficulties are related to the absence, to date, of safeguards and clear and binding legal provisions which ensure that FIUs' information passed on to law enforcement agencies or prosecutors is not improperly used as evidentiary material in a legal proceeding without duly triggering a prior MLA initiative. In fact, as said, the information would be forwarded by the FIU with the explicit limitation that it is not to be used as evidence outside of a proper Mutual Legal Assistance procedure and without being subject to the conditions applicable in that context. This limitation, in fact, would be attached to the consent granted by the foreign counterpart FIU that has provided the information through the FIU-to-FIU cooperation channel. Despite this inherent restriction at the basis of the FIU-to-FIU cooperation, it may well be that, in the absence of explicit provisions on this matter in domestic or EU legislation, neither the terms of the foreign FIU's consent nor the limitations stemming from it as specified by the domestic FIU are binding upon the law enforcement bodies or the prosecutors receiving the information.

In other words, police agencies and magistrates, based on applicable substantive and procedural rules to which they are bound in conducting criminal investigations or legal proceedings, may well be allowed, or even required, to use any information that becomes available as a means to build the evidence necessary in support of the investigation and come to conclusions in terms of, for

example, seizure, conviction or confiscation, even regardless of the source of the information and of the possible conditions attached to its use, in the different FIU-to-FIU cooperation context.

The freedom that in many jurisdictions prosecutors enjoy (or, rather, are required to use) to produce actionable evidence would in these cases not be constrained by previous agreements reached between different agencies, such as FIUs, on the exchange and use of the information made available. The prosecutor would simply be a third party with respect to the FIUs' agreement about the consent and the attached limitations and not bound by them.

The absence of safeguards and limitations as to the use of foreign FIUs' information in legal proceedings in conformity with the terms of the consent is certainly a strong deterrent for FIUs to grant the consent in the first place. Respondents have flagged these concerns very clearly in their submissions. Some remarks focus on the loose of any control by the providing FIU on how the information exchanged will be used and if this use will be in conformity with the consent and with possible limitations or conditions specified therein. Very often, let alone controlling the information, not even feedback is available on the use that has been made of it. Cases where forms of misuse have been detected[206] are also referred to by respondents; it is observed that these cases are taken into consideration in subsequent exchanges with the interested counterparts and can, in extreme circumstances, lead to refusals to share further information.

On the other hand, responses also highlight that, once the FIU has forwarded the information obtained from foreign counterparts to other domestic agencies with all necessary caveats and safeguards, it also may lose the control on this information[207] and cannot be held responsible for possible misuse by third parties[208].

On this delicate matter of ensuring that FIUs' information is used in conformity with their authorization, also when it is passed on to third parties, it is necessary to consider if dedicated measures or provisions should be introduced. At stake here is the effectiveness of FIUs' cooperation in relation to their capacity to support investigations and prosecutions, the possibility of secure exchanges of information between FIUs, the appropriate coordination between the FIUs' channels of cooperation and the police and judicial international cooperation mechanisms.

10.9.4 Use and dissemination for intelligence purposes

Use and dissemination for intelligence purposes, besides the analysis performed by the requesting FIU and also in the context of subsequent investigations should in principle always be possible. The dissemination for such further "intelligence purposes" should be considered as strictly inherent to the general dissemination function of FIUs and should follow as a natural consequence of the initial exchange.

As already argued, such exchange would otherwise be deprived of any practical use. In fact, the sharing of information and the analysis function are instrumental to dissemination; more specifically, analysis not followed by the dissemination of their positive outcomes, supported by either domestic or foreign information, is meaningless. For these reasons, the consent for the ordinary dissemination by the FIU for further intelligence should be presumed as implicit in the provision of the information through FIU-to-FIU cooperation. Rather than a "prior consent", the

[206] That is, unauthorized use beyond what had been consented or undue further dissemination.
[207] Similarly to what may happen for the information related to domestic STRs/SARs and analysis.
[208] In this context, an exemption of responsibilities should also be considered for FIUs in cases of improper use of foreign information by domestic agencies to which it has been disseminated if the terms of the consent have been complied with and all applicable conditions and appropriate safeguards have been put in place.

possibility should be envisaged to deny the further use and dissemination for intelligence purposes in limited exceptional circumstances.

On this note, it is important to stress that responses to the Survey have expressed the view that the consent should be provided together with the information, at very initial stage of the exchange, thus facilitating and speeding up both the FIU-to-FIU cooperation and the domestic dissemination (the need for a separate and subsequent request for consent would in fact be avoided).

CHAPTER 7

COOPERATION WITH NON-FIU COUNTERPARTS ("DIAGONAL COOPERATION")

1. Introduction. "Diagonal" cooperation with foreign EU non-counterparts; features, modalities, difficulties

Besides the exchange of information among themselves, FIUs (like other authorities) can be called on to cooperate with foreign agencies that are not FIUs. Similarly to what is routinely carried out at the domestic level, where FIUs share information with other bodies within their own countries, FIUs could as well entertain forms of cooperation with non-FIU counterparts established in other countries.

Cross-sectorial cooperation between competent authorities of different jurisdictions that do not exercise the same functions domestically (and which are not, therefore, direct "counterparts" reciprocally) is proving increasingly useful to support those functions, especially when these, although different and separately regulated both in domestic laws and international standards, are interconnected or otherwise focus on the same or related matters.

For what concerns FIUs, forms of "diagonal" cooperation with foreign agencies that exercise different functions are pursued (to the extent allowed by the existing legal framework: see the following paragraphs) particularly in cases where either the functions of these latter agencies can receive support from STR/SAR information or, vice versa, when the FIUs' analytical activities to uncover money laundering, predicate offences or terrorist financing can benefit from information held by foreign non-counterparts. In this perspective, forms of diagonal cooperation between FIUs and foreign non-counterparts can be particularly useful to pursue investigations or supervisory actions, as well as to invigorate and further substantiate the FIUs' analyses.

For example, it is important to recall that supervisors, particularly based on provisions introduced by EU directives in the financial sector, have an increasing need to obtain STR/SAR information in the context of the "fit and proper" tests conducted in prudential supervision, especially for licensing or authorization purposes in order to prevent criminals, or other otherwise unfit individuals, from acquiring significant shares or managing positions or misusing in other ways regulated entities. This STR/SAR information may be obtained by supervisors both from within their own jurisdiction, through cooperation with the local FIU and from other countries (when, for example, the applicant is a foreign resident or national or has otherwise interests abroad), through international diagonal cooperation[209].

[209] As we will see later in this Chapter, this can be achieved in practice through different modalities, either directly through exchanges between supervisors and foreign FIUs, or indirectly, through the supervisors or the FIUs of the countries involved. In the following paragraphs we will also argue that the transmission of sensible STR/SAR information, and the potential relevance of the underlying cases to uncover money laundering or terrorist financing activities through FIUs' analysis, bring strong elements in favor of using the secure and protected FIU-to-FIU communication channels and to always appraise, in diagonal exchanges, the FIUs of the interested countries.

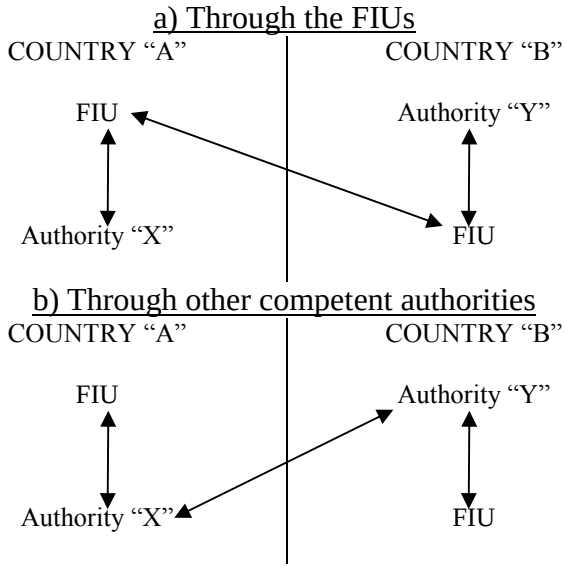
Similar considerations apply, quite obviously, for investigative activities conducted by police agencies in relation to transnational crimes. While FIUs ordinarily cooperate and share information with their domestic law enforcement agencies in various modalities[210], forms of cooperation with foreign police agencies are equally useful in relation to investigations ongoing abroad.

On the other hand, it is also important to bear in mind that FIUs' information on STRs/SARs and their analysis is particularly sensitive and should be adequately protected against too extensive uses via excessively broad forms of diagonal exchanges with foreign non-FIU agencies. One important caveat is, for example, that, in line with indications provided by the Egmont Group, information on STRs/SARs, when exchanged diagonally, should always be channelled through the FIU-to-FIU cooperation mechanisms (so that the information is securely protected and the interested FIUs always informed).

In fact, diagonal cooperation can be carried out according to different modalities and through different channels. "Indirect" forms of exchange are based on the information being channelled through third party agencies, in the country of the requested authority, in that of the requesting authority or in both, before reaching the final intended recipient. These are cases where FIUs' information is exchanged by the FIU with non-FIU foreign counterparts either through the FIU-to-FIU communication channels (therefore involving the FIU of the country of the non-counterpart agency) or through another agency in either of the countries involved. For example, to exchange information with a foreign supervisor, an FIU could (or should, depending on the applicable legal framework) channel the communication through the FIU of the country of the supervisor (which forwards the request or response to the latter) or through its domestic supervisor (which forwards the request or response to its foreign counterpart).

Therefore, indirect diagonal cooperation for the exchange of STR/SAR information could take one of the forms sketched out below.

FIUs' indirect diagonal cooperation



[210] These typically include dissemination, either spontaneous or on request, and other exchanges of information for the FIU's analysis or for police investigations.

It can be argued that, since diagonal exchanges involving FIUs relate to STR/SAR information (either received through disclosures or acquired through analysis), the FIU of the country where the non-counterpart is located should always be involved and informed. This would allow it to take account of the case as potentially relevant for its own analysis and, at the same time, share possible additional information (with the foreign FIU, with the domestic agency involved in the diagonal exchange or with both). Moreover, using the FIU-to-FIU communication mechanisms would allow the application of the dedicated secure means of exchange which ensure that sensible STR/SAR information is kept adequately protected. For these reasons, the indirect forms of diagonal cooperation, depicted above in a), seem preferable with respect to direct diagonal cooperation, based on direct communications between the FIU and the foreign non-counterpart.

The exchange of information between FIUs and foreign agencies that are not counterparts would require, and certainly benefit from, an appropriate legal framework specifically providing for appropriate forms of diagonal cooperation and regulating the exchanges. This legal framework, while of course implemented through national laws, should be firmly rooted in dedicated EU provisions, so as to establish a common system of cooperation based on uniform modalities and conditions allowing the dialogue between different agencies across Member States (see more on this in paragraphs 7 and 8).

Despite diagonal cooperation being increasingly practiced by FIUs and other competent authorities[211], it appears to be still under-utilised and subject to significant difficulties and uncertainties. This may also depend on existing different approaches and conditions across Member States which, in turn, depend on the absence of a uniform common framework at the EU level.

While the fourth Directive neither foresees nor regulate international diagonal cooperation for AML/CFT purposes, the 2012 FATF Recommendations[212] have introduced a requirement for countries to permit indirect diagonal cooperation, (described as forms of exchange where the information passes from the providing authority through one or more domestic or foreign agencies before being received by the recipient authority). Differently, direct forms of exchange between foreign non-counterparts (direct diagonal cooperation) are only "encouraged" and, therefore, they are not mandatory[213]. The FATF standards also establish that, regardless of which pattern is chosen for the exchange, this should always take place "in a secure way and through reliable channels or mechanisms".

It is also important to stress that, unlike from the traditional FIU-to-FIU cooperation which in all cases embodies a duty for the FIUs involved to respond to requests, under the FATF Recommendations diagonal cooperation has to be allowed by countries (under the "indirect" form, as countries are only "encouraged" to consider the direct type of diagonal sharing) but it does not entail an obligation for FIUs to share information with foreign non-counterparts. FIUs, based on domestic laws, should be empowered but not compelled to cooperate diagonally; therefore, responses to requests for information from foreign non-counterparts should always be possible for FIUs (in the indirect form) but are not mandatory for them.

The essential features of diagonal cooperation for FIUs, in light of the FATF and Egmont standards and guidance, can be summed up in the following points.

[211] Responses to the survey seem to confirm this, although they also point out several difficulties and frequent cases where FIUs are not in a position to engage in such forms of cooperation. See paragraph …

[212] See the Interpretive Note to Recommendation 40, sections 17 and 18.

[213] A similar approach is followed by the Egmont Group in the "Operational Guidance for FIU Activities and the Exchange of Information", issued in 2013.

- Countries should permit indirect diagonal cooperation and can allow direct diagonal cooperation.
- FIUs should be empowered by law to exchange information indirectly with foreign non-counterparts and could be empowered to exchange this information in a direct manner.
- Differently from direct cooperation with counterpart FIUs, diagonal cooperation (both direct and indirect) is not an obligation; this means that FIUs should be able to decide, also on a case-by-case basis, whether or not to exchange with foreign non-counterparts and which channels to use[214].
- STR/SAR information exchanged diagonally should be adequately protected, similarly to information shared through the traditional FIU-to-FIU cooperation.

This last point may entail that FIUs' communication channels should also be used for diagonal exchanges, thus also allowing the FIUs of the countries involved to be informed about the case for any appropriate follow up within their competences.

The survey shows that, lacking a specific EU framework on this matter, not all EU FIUs have the capacity to entertain international diagonal cooperation. In many cases, due to the absence of a domestic legal basis, the objective of exchanging information with foreign non-counterparts can only be achieved indirectly, by means of ordinary inter-FIU sharing followed by the consent to use or disseminate the information provided "diagonally". However, these forms of cooperation encounter obstacles and limitations (besides those discussed in Chapter 6, paragraph 10 limiting the capacity to authorize further use or dissemination) associated with the lack of capacity for many FIUs to allow the use of the STR/SAR information provided for purposes other than analysis or investigation (e.g. supervisory actions) or for the ascertainment of criminal activities other than money laundering or terrorist financing[215].

In addition, difficulties are determined by the different mechanisms and channels that can or must be used by FIUs to exchange information diagonally: while some stick to the FIU-to-FIU means of communication, others liaise directly with foreign non-counterparts (especially police agencies: see paragraph 3.1 later). This can raise issues of adequate involvement of all interested FIUs and of adequate protection of STR/SAR information.

An adequate legal basis at the EU level, providing for forms of diagonal cooperation for FIUs and regulating applicable mechanisms and modalities, would allow to overcome many of these obstacles and increase the use of effective diagonal cooperation, in keeping with the need to maintain adequate safeguards.

2. Capacity to exchange information with foreign counterparts that are not FIUs

The majority of EU FIUs stated that they have the capacity to exchange information with non-FIU counterparts. This capacity is only in some cases rooted in dedicated explicit legal provisions in domestic laws (only 12 respondents have indicated that diagonal cooperation is expressly provided for by the law). In other cases, EU FIUs can entertain forms of diagonal cooperation as these are not

[214] The regime of indirect diagonal cooperation mirrors closely that applicable to the dissemination upon request at the domestic level. While the two forms of exchange refer respectively to the international and to the domestic domain, they both have in common the fact that the FIU sends or exchanges information with non-FIU counterparts. Other common elements are that both dissemination upon request and international diagonal cooperation are subject to national law, which can add provisions taking account of the FATF framework, and that FIUs' independence should be safeguarded, especially by avoiding forms of systematic or mandatory dissemination or exchange.

[215] The considerations in Chapter 6 on the "purpose limitation" underlying and defining FIUs' cooperation should be recalled here.

prohibited by the domestic legislation which, on the contrary, empowers these FIUs to exchange information generally with foreign agencies (of whatever nature). Overall, 21 respondents have indicated that they can engage in diagonal cooperation, either based on an explicit legal recognition or on implicit authorising provisions[216].

For example, a respondent has pointed out that, although a dedicated legal basis for international diagonal cooperation is lacking in its country, this cooperation is carried out frequently, particularly in the following instances:

- "cases where [the FIU] requests or provide information to or on behalf of law enforcement agencies or prosecutors; this is particularly important in cases where investigations and prosecutions have already been started and run in parallel with financial analyses; FIUs' cooperation is in such cases often conducive to ensuing mutual legal assistance";
- "cases where information is exchanged with foreign supervisors, or provided to domestic supervisors; these are instances where STR or other analytical intelligence is needed to run 'fit and proper' tests underlying, for example, licensing, authorisation or other vetting processes".

Another respondent has clarified that its capacity to cooperate diagonally is based on national provisions which, although not explicitly mentioning these forms of cooperation, are formulated broadly and empower the FIU accordingly: "These regulations do not indicate explicitly that the exchange of information should be conducted only with FIUs and allows our FIU to exchange information on ML/TF activities with other international authorities".

Some respondents highlight that cases of diagonal cooperation are highly unusual or have never occurred. Others flag that diagonal exchanges only take place through law enforcement international communication channels (e.g. Europol, Interpol, liaison officers, international letters of request) and only concern police information.

It is important to emphasize that a significant number of FIUs seem to lack the capacity to provide forms of diagonal cooperation entirely. Based on responses, this seems to be a consequence of two combined factors: a) the absence of legal provisions empowering the FIU, explicitly or implicitly, to share information with foreign non-counterparts; b) the constraints in providing the consent to foreign FIUs to further use or disseminate the information shared with them for purposes other than the analysis or investigation[217] of money laundering or terrorist financing cases (purpose limitation).

3. Direct and indirect channels used for diagonal exchanges

The vast majority of EU FIUs that can engage in international diagonal cooperation with foreign non-FIU counterparts do so through indirect means, that is through the FIU-to-FIU mechanisms. These are cases where STR/SAR information are first transmitted by an FIU to the FIU of the country where the interested non-counterpart is located and then forwarded to such non-counterpart, based on the appropriate consent granted by the providing FIU.

Making use of these diagonal communication mechanisms, as already indicated, allows the FIUs of the countries involved to be involved in the case for which the cooperation is sought, as well as of the information needed and exchanged, and informed about its features and possible relevance. As also said, however, these indirect modalities of diagonal cooperation are in several cases dependent on the existence of dedicated provisions on diagonal cooperation in domestic laws and on the use of

[216] In most cases, these latter FIUs can provide diagonal cooperation only through ordinary FIU-to-FIU communication, followed by the consent to further disseminate the information to other interested agencies.
[217] Usually referred to in practice under the broad label of "intelligence".

ordinary channels of FIU-to-FIU cooperation for reaching non-FIU counterparts by means of the required prior consent for the further use or dissemination of the information shared (see paragraph 7 on the legal basis for a description of the limitations inherent to this approach).

For example, a respondent highlights that "any communication with non-counterparts takes place through FIU communication lines". This respondent also confirms that it is up to the FIU to assess if the exchange is compliant with applicable domestic provisions regulating the FIU's cooperation (which do not explicitly cover diagonal cooperation).

Along the same lines, another respondent also confirms that "provisions of the [AML] Law regulating international exchange of information apply in these cases as well, giving consent to the requesting FIU to disseminate information to non-FIU counterparts as intelligence for AML/CFT purposes only".

Eight FIUs have stated that they can exchange information with foreign non-counterparts directly, i.e. outside of the indirect FIU-to-FIU cooperation channels. Interestingly, these respondents are either police FIUs or FIUs that perform also additional supervisory tasks. Although the information gathered through responses do not allow to draw firm conclusions on this point, it appears that police FIUs are, at least in some cases, allowed to share STR/SAR information directly with foreign law enforcement agencies without passing (or having to pass) through FIU-to-FIU cooperation mechanisms.

As previously noted, some respondents have indicated in this respect that information can be in fact provided to foreign law enforcement bodies through police cooperation procedures and channels; direct communications with Europol and Interpol are also referred to in this context. A respondent has specified that these forms of direct communication with non-FIU counterparts are only possible in relation to police information and not for the exchange of financial information.

As indicated, other instances of direct cooperation with foreign non-FIU counterparts are reported by respondents that also perform supervisory tasks. These forms of cooperation seem related to the direct exchange of information with foreign supervisors on matters concerning the compliance with AML/CFT measures by obliged entities, rather than the sharing of STR/SAR information for the identification or analysis of potential money laundering or terrorist financing activities.

On this note, for example, a respondent has indicated that, "although exchanges of information with non-FIU counterparts in practice take place indirectly through FIU channels, the [AML Law] does not preclude the [FIU] from exchanging information directly with non-FIU counterparts. The [FIU] has AML/CFT supervisory powers and thus certain exchanges of information with foreign supervisors would occur within this context without the need of informing the FIU of the jurisdiction of the counterpart supervisory authority".

Another respondent emphasizes that, "as a supervisory authority or as the authority enforcing targeted financial sanctions, [the FIU] can exchange information directly with counterparts"; as also indicated by the same respondent, this cooperation "is not carried out in the capacity of an FIU".

Differently from what has been indicated above about direct exchanges between FIUs and foreign police bodies, these forms of direct cooperation on supervisory issues do not normally concern STR/SAR information, as they focus on compliance aspects for regulated entities. It may also be argued that these exchanges do not qualify as FIUs' diagonal cooperation, in the logic of international standards in this matter, precisely because neither of the parties involved act an "FIU".

3.1 Issues in the direct "diagonal" cooperation for the exchange of police information

In the instances recalled in the previous paragraph, where responses have highlighted that some law enforcement FIUs are able (or required) to share information directly with non-FIU foreign police counterparts, the question arises of whether in such circumstances these FIUs act as such or perform other, law enforcement cooperation activities, which are carried out through forms and modalities different from those applicable to FIUs' cooperation and are regulated under a separate regime.

The former situation, of FIUs acting as such and exchanging in their role information on STR/SAR with foreign law enforcement agencies through police or judicial channels, more than an instance of direct diagonal cooperation with foreign non counterparts, may be regarded as a case of limitation or constrain to the use of the FIU-to-FIU cooperation system and mechanisms.

In fact, all FIUs, regardless of their nature and including those that have a law enforcement status, should be able (and required or, at least, expected) to make use of the FIU-to-FIU exchange mechanisms and procedures for sharing and obtaining STR/SAR information, be this information administrative, financial or law enforcement. Reverting to law enforcement cooperation by FIUs that exchange police information related to STR/SAR may entail a derogation or a limitation to ordinary FIU-to-FIU cooperation which, in accordance with EU provisions, should include also law enforcement information. The more so (as will be discussed shortly), as responses show that these exchanges are ordinarily conducted without even appraising the FIU of the foreign country involved (that is, the country of the police agency which is directly approached by the foreign FIU).

While the findings of the survey on this point appear surprising, further analysis would be needed to confirm whether there are limitations or derogations to the use by FIUs of their ordinary cooperation mechanisms and their extent. More particularly, a better understanding is needed of whether the FIUs exchanging information directly with foreign police bodies do so in the context of analysis of STRs/SARs or to the aim of fostering investigations being conducted (either by the same FIUs in context of additional law enforcement tasks or by the foreign police correspondent).

In the former case, it would typically be acting as an FIU in discharging its core analytical functions; the direct interlocution with foreign police bodies, rather than with the local FIUs, may represent in this context a deviation from the legal and operational framework designed for FIUs and for their cooperation. In the latter case, where the direct exchange is conducted in support of law enforcement activities (either conducted by the same FIU or by the foreign police agency seeking assistance), the FIU may not be acting as such, as the function performed is not the analysis of suspicions, but may be rather exercising additional, non-FIU, police tasks assigned to it under domestic laws.

Also in this context, however, if the direct exchange involves STR/SAR information, or intelligence developed through FIU's analysis, the necessary distinction between FIUs' cooperation (which is in fact typically dedicated to the sharing of this information) and police cooperation activities (aimed at fostering investigations), the two being separately regulated and conducted through different modalities and channels, may become blurred. This can be at the expense, and to the detriment, of the separateness of the former from the latter and to the autonomous conduction of FIUs' cooperation with respect to law enforcement cooperation.

This issue of keeping the FIUs' cooperation distinct and autonomous in cases of direct diagonal exchanges carried out by police FIUs becomes particularly prominent in light of the following circumstances. Responses clearly show that in most cases the FIUs that send information directly to

foreign law enforcement counterparts do not appraise or notify the FIU of the country concerned, which therefore may remain unaware of the exchanges and of the underlying cases (see the following paragraph), even when the information shared is about STRs/SARs pertaining to its country. The more so, as in many instances the FIUs of the interested countries do not have a law enforcement status and, therefore, may not be informed indirectly about the case through domestic cooperation or coordination channels.

"Confusion" and overlaps between the FIUs' analytical functions, and the related international cooperation activities, and law enforcement activities on the same facts arise also, as seen, as regards the performance of "analysis" (which in some cases does not seem separate from "investigation": see particularly Chapter 5) and of FIUs' cooperation in its support (which is often conditioned or limited due to ongoing law enforcement activities: see Chapter 6, par.1.4).

In light of these considerations, the issue of the distinction between FIUs' and law enforcement functions, when these are assigned to the same unit in charge of both, appears to be particularly relevant. Its importance is strictly and directly related to the need that FIUs' functions of analysis and international cooperation be kept separate and autonomous. As regards particularly the area of international cooperation, it is important to ensure that FIUs are not unduly limited in exchanging information relevant for analysis, even when this information has a "police" nature or there are investigations or legal proceedings underway[218].

4. In case of direct exchanges, are the FIUs of the interested Member States informed?

When FIUs' diagonal cooperation assumes indirect forms, that is information (requests or responses) is passed on to or from the final recipient through the FIU of the interested country, this FIU is appraised of the exchange and of the underlying case. As said, this allows it to consider the case for possible follow-up through own analysis and for possible additional information sharing (either complementing the ongoing diagonal exchanges or initiating a separate direct dialogue with the counterpart FIU). Differently, in cases of direct diagonal exchanges, the FIUs of the country where the non-FIU counterparts are located are not involved in the cooperation activities and may not receive information about its occurrence and context.

In such cases, it is particularly important that the FIU that engages in direct forms of diagonal cooperation with foreign non-counterparts appraises the FIUs of the same countries about the ongoing cooperation activities and of the underlying cases. This is particularly needed when the information exchanged is related to STRs/SARs or is otherwise connected with suspicious cases of money laundering or terrorist financing or with analytical activities.

Unfortunately, out of the 8 FIUs that have indicated that they can liaise directly with foreign non-counterparts, only 3 have confirmed that they also inform the FIUs of the interested Member States about the exchanges and the underlying cases.

In some of these instances the FIU may be prohibited from disclosing circumstances concerning the direct diagonal exchange. In other situations, this issue seems not regulated and the FIU may have some room for discretion. For example, one of these respondents flags that, "depending on the case, the FIU of the interested Member State may be informed of the exchanges".

As already highlighted, the FIUs that can exchange information directly with foreign non-counterparts are in most cases law enforcement FIUs. More particularly, based on responses, these

[218] The considerations and analyses developed in Chapter 6 on these aspects can be recalled here.

FIUs can share police information with law enforcement bodies in other countries. This information may well concern possible money laundering or terrorist financing cases and can also originate from STR/SAR or related analysis. In the previous paragraph, the issue of possible limitations to FIUs' cooperation deriving from the direct use of police channels to transmit STR/SAR information has been flagged; as also already emphasized, it would important to ensure that when FIUs are allowed, or required, to forward to foreign non counterparts information which is potentially relevant for the identification of money laundering or terrorist financing in other countries, or is otherwise related to STRs/SARs, the FIUs of those countries be informed. As said, this would allow such FIUs to possibly follow-up on the underlying cases by, for example, conducting own analysis and complementing the exchanges of information underway. Coordination between different activities on the same cases would also be facilitated, both at the domestic and at the international level.

Direct sharing of information is also carried out by FIUs in the exercise of supervisory tasks assigned to them by their domestic legislations. Although responses show that also in these cases the FIUs of the countries where the foreign non counterparts are located may not be informed of the direct diagonal exchanges, it is important to recall that these exchanges are normally neither related to potential money laundering or terrorist financing cases nor do they stem from STRs/SARs in their countries.

5. Information that can be shared through diagonal cooperation

In most cases, the absence of a legal basis specifically underpinning diagonal cooperation, its scope and content, also leaves areas of uncertainties as regards the information that FIUs can exchange with foreign non-counterparts. On this issue, the responses highlight three main elements for consideration.

As a first point, in general, the scope and range of the information available for diagonal cooperation are the same as those related to the information that can be exchanged through FIU-to-FIU cooperation. As seen, in fact, in many where cases the FIUs' capacity to cooperate with foreign non-counterparts is rooted into domestic provisions that empower them to share (the same) information generally with foreign agencies (that is, beyond FIUs), these provisions are broadly formulated. Some limitations on the FIUs' capacity to share certain categories of information with foreign non-counterparts may however derive from the way in which the domestic provisions setting the scope of the information powers are drafted. For example, FIUs do not seem in general able to exercise their own domestic powers to obtain information on behalf of foreign non-FIU counterparts. Also, depending on the wording of national provisions, certain categories of information may not be available for diagonal sharing.

For example, a respondent has indicated that, "based on current legislation, police information may not be obtainable on request of a foreign entity which is not an FIU". Existing constraints and limitations to the access to financial information and databases can also be recalled here, as they can be amplified in diagonal cooperation contexts.

Secondly, the general "purpose limitation" which delimits the FIUs' capacity to cooperate internationally plays a particularly important role in diagonal exchanges. As discussed in Chapter 6, FIUs can engage in international cooperation and exchange information in relation to suspicions of money laundering, predicate offences or terrorist financing (not to outright evidentiary material on any type of criminality) and in support of analytical or "intelligence" activities (not of law enforcement or prosecutorial actions).

While this general purpose limitation does not normally affect FIU-to-FIU cooperation (as in fact FIUs carry out analysis concerning suspicious money laundering or terrorist financing activities), it can pose significant limits to the FIUs' capacity to provide cooperation to non-FIU foreign counterparts through diagonal cooperation. These counterparts, in fact, do not perform analysis of suspicions (as this activity is typical of FIUs) and do not even necessarily focus specifically on money laundering, its predicate crimes or terrorist financing. As seen, diagonal cooperation is usually requested to FIUs by law enforcement agencies in need of information to support investigations or legal proceedings (not only related to money laundering or terrorist financing) or by supervisors.

Responses show that the purpose limitation that underpins FIUs' cooperation poses significant restrictions to the FIUs' capacity to share information with foreign non-counterparts.

For example, respondents emphasize on this point that, "in accordance with [the AML law] the information can be used only for prevention and counteraction of money laundering", specifically "for intelligence purposes only" and that the FIU "may only share information that is connected with money laundering, associated predicate offences or terrorist financing pursuant to its domestic laws".

The third element that needs to be considered as regards the scope of the information that can be shared with foreign non-FIU agencies is that, as shown by responses, the capacity to provide diagonal cooperation is subject to the same conditions and limitations that apply in general to the FIU-to-FIU sharing. Due, again, to the absence in most cases of an ad hoc legal basis specifically underpinning diagonal cooperation, common provisions on FIUs' capacity to cooperate are applied to both ordinary FIU-to-FIU exchanges and diagonal forms of sharing. These latter, as said, seem to be subject, in particular to the "prior consent" regime referred to possible further use or dissemination of the information exchanged.

The most significant conditions and limitations applicable to FIUs' cooperation, as specifically discussed in Chapter 6, are related to the existence of investigations or legal proceedings in the country of the requested FIU, the need for prior authorizations or clearance, the involvement of tax matters, the requirement that a predicate offence be identified and correspond to an offence which is also criminalised domestically.

Several respondents confirm that diagonal cooperation is carried out "based on the same principles and conditions applicable for the FIU-to-FIU exchange" and that "the same limitations apply as in correspondence with other FIUs".

More specifically, some respondents highlight that they cannot provide diagonal cooperation in cases where ongoing investigations or national security" can be impacted. An FIU recalls that it can refuse the exchange particularly if: "(a) in its opinion such disclosure could lead to causing prejudice to a criminal investigation in course in [the Country]; or (b) due to exceptional circumstances, such disclosure would be clearly disproportionate to the legitimate interests of [the Country] or of a natural or legal person; or (c) such disclosure would not be in accordance with fundamental principles of [national] law".

6. Possible use by foreign non-counterparts of the information shared

Similarly to what has been observed in the previous paragraph about the limitations concerning the scope and types of information that FIUs can provide to foreign non-FIU agencies, also the use that these counterparts can make of the information received is limited in accordance with national legal

bases underpinning in general FIU-to-FIU cooperation and specifically by the purpose limitation. Respondents, therefore, flag that the same rules and constraints apply to the use of information transmitted to non-counterparts as those applicable to traditional exchanges between FIUs. In this context, most FIUs confirm that the information can only be used for "intelligence purposes" (that is, outside of formal prosecutions or legal proceedings) and in relation to investigations on money laundering, predicate crimes or terrorist financing (which seems to rule out the use of STR/SAR material for supervisory purposes).

On this last point, a respondent has indicated that, "as regards the exchange of information with [foreign] supervisory authorities, the [FIU] states that the purpose for exchanging information with supervisory authorities should be that of ensuring that the financial system or other systems are not misused for criminal purposes and of safeguarding the integrity of such systems". This respondent is an FIU which is also in charge of supervisory functions and it is not clear whether the information referred to in the response is related to this function or can also pertain to STRs/SARs and their analysis.

As already recalled, the application of the purpose limitation and of the constraints generally related to FIU-to-FIU cooperation are likely to limit significantly the scope of diagonal cooperation, notably as regards the use of the information that can be done by foreign receiving agencies which, not being FIUs, perform tasks different from the analysis on suspicious money laundering or terrorist financing cases.

These limitations are particularly recalled by a respondent which points out that the information provided diagonally can only be used "for the purposes related to, directly or indirectly, AML/CFT" and that, to ensure that this limitation is understood and fulfilled by foreign non-counterparts, "some 'caveats' usually accompany the diagonal exchanges", in the form of the following requirements:

- "The use of the information shall be confined to internal analytical purposes closely related to ongoing supervisory purposes, in order to assess the existence of eligibility or integrity requirements;
- any mention of reference to the existence of STRs and their contents shall be excluded in formal internal analysis acts and, a fortiori, in those having external significance or intended to be notified to third parties or published;
- disclosure or further use or dissemination of information to the persons concerned or any other public or private subject shall be prohibited, both in the preliminary as well as later stages, including any access to information, procedures or contentious proceedings;
- the information can be used only for the specific purposes for which it was requested or provided;
- the information must be processed and stored (within the temporal limits of the applicable data protection provisions) with adequate safeguards for security and confidentiality".

7. Lack of appropriate legal basis in support of diagonal cooperation

As noted in previous analysis, while the majority of the EU FIUs have confirmed that they can engage in diagonal cooperation (under the forms and modalities highlighted earlier in this Chapter), this capacity is in many cases based on domestic provisions about international cooperation that are formulated in sufficiently broad terms but which do neither address diagonal cooperation as such nor regulate it specifically. In fact, only a minority of respondents have indicated that diagonal cooperation is expressly provided by their national laws, despite this form of information sharing

being required by the FATF Recommendations since 2012 (at least through indirect modalities: see paragraph 1).

A respondent has informed that "diagonal cooperation will be explicitly provided by law when transposing the 4th EU AML/CFT Directive" and that "the principles of the diagonal cooperation laid down in the Egmont Group of Financial Intelligence Units Principles for Information Exchange between Financial Intelligence Units will all be observed".

Many respondents flag that, although dedicated provisions on diagonal cooperation are lacking, this is implicitly allowed by general provisions empowering the FIU to share information with foreign agencies (either FIUs or non-FIU entities), as well by provisions on the possibility to provide the consent to another FIU for the dissemination of the information exchanged to other, non-FIU foreign agencies (this is why in many cases diagonal cooperation is carried out in indirect forms; see further considerations on this in the text below).

In light of responses, as a consequence of the absence of a legal basis in several countries (and, in the background, of a uniform framework at the EU level), diagonal cooperation is often only implicitly allowed and is left unregulated in its possible modalities. This may determine difficulties in ensuring that adequate cooperation in this area can be provided to a sufficient degree. Even when it can be provided, the lack of a dedicated comprehensive legal framework may lead to differences and discrepancies which, in turn, may make the dialogue difficult and uncertain, both between FIUs (for example, as regards their involvement in direct diagonal exchanges: see paragraph 3 above) and between FIUs and non-FIU foreign counterparts.

Although responses do not explicitly mention data protection restrictions, it is reasonable to assume that, in the absence of specific provisions allowing to share information with foreign agencies, these restrictions also play a role in preventing FIUs from engaging in diagonal cooperation.

Responses show that, in the absence of dedicated domestic provisions, diagonal cooperation is often carried out by FIUs through the ordinary FIU-to-FIU information sharing and based on the provisions regulating it: in accordance with the usual "prior consent" approach, in cases where the information has to reach a final recipient that is not the correspondent FIU, the initial FIU-to-FIU exchange is followed by an ad-hoc authorization to forward the information, "diagonally", to the intended non-FIU recipient.

Several responses provide examples of diagonal cooperation carried out, indirectly, through initial FIU-to-FIU exchanges followed by the consent for further dissemination. A respondent has indicated that "within its legal basis, not only [the FIU] is able to (and does, in practice) grant consent to its foreign counterparts to further use and share the information provided for law enforcement and prosecutorial purposes; also, it can consider passing information on to foreign authorities which are not FIUs ("diagonal" cooperation). In such cases, in accordance with the FATF and Egmont standards, however, the diagonal exchange is done indirectly, that is the foreign FIU of the interested state is always appraised and the information is channeled through it".

Under this approach, in the absence of ad-hoc legal provisions, diagonal cooperation, more than an autonomous form of information sharing, is a "by-product" of ordinary FIU-to-FIU cooperation, resulting from the exchange of information between FIUs followed by the consent to forward such information to another agency as the intended recipient in the country of the receiving FIU. As a consequence, the diagonal prolongation of the FIU-to-FIU exchange through the dissemination to further agencies remains subject to general domestic provisions regulating FIUs' cooperation, based on case-by-case considerations (taking account, for example, of the recipient and of the intended

use of the information transmitted) and subject to the conditions and limitations applicable to the further dissemination and use of the information shared[219].

This may entail that diagonal cooperation:

- may be entertained occasionally, rather than systematically, depending on factors such as the intended use or the recipients of the requested information (e.g. supervisors, tax agencies, law enforcement bodies for non ML or TF-related investigations);
- may be subject to conditions and limitations applicable to FIU-to-FIU cooperation, including those related to both the initial exchange and to the ensuing consent for further use or dissemination; in this respect, as previously discussed, the limitations deriving from the "purpose limitation" underpinning FIUs' cooperation are likely to play a particularly significant role;
- may be dependent on differences in conditions or limitations in place in different countries, which may determine difficulties and uncertainties in exchanges and also trigger the reciprocity condition, with adverse effects on the extent of cooperation[220].

8. Conclusions and proposals

The analysis in this Chapter has highlighted several outstanding issues surrounding the capacity of EU FIUs to carry out diagonal cooperation. These issues, recapped below, appear to require appropriate regulation on some key aspects to be adequately tackled. This regulation should be implemented at national level against a uniform background at the EU level to ensure that common approaches are followed and effectiveness is achieved.

First of all, diagonal cooperation frequently lacks a legal basis in EU Countries. As discussed in previous paragraphs, this entails that in these Countries, while several FIUs lacks the capacity to engage in this form of cooperation entirely, others can share information with non-counterparts either based on implicit assumptions or utilising the same provisions applicable to FIU-to-FIU cooperation and adapted to accommodate forms of indirect diagonal sharing based on an "ad-hoc" consent following the initial sharing. In both cases, diagonal cooperation rests on uncertain grounds and finds significant constraints stemming most of all from the "purpose limitation" which ties FIUs' cooperation to the pursuance of "intelligence purposes" in the prevention and fight of money laundering and terrorist financing.

In this context, while in principle nothing seems to prevent FIUs from requesting foreign non-counterparts for information useful for the analyses of the former, the FIUs' capacity to contribute to other authorities' activities which could benefit from STR/SAR information appears limited. More particularly, due to its narrow scope, diagonal cooperation cannot be pursued in many cases (at least, not systematically) in support of law enforcement activities (especially in relation to investigations or prosecutions not related to money laundering or terrorist financing), fiscal purposes or supervisory actions carried out by competent authorities in other countries[221].

Of course, as previously recalled, it is important to ensure that sensible STR/SAR information is not overly exposed and unduly or excessively divulged through indiscriminate inter-agency sharing

[219] See, on this, the analysis in previous paragraphs in this Chapter.
[220] The considerations and examples in previous paragraphs on limitations to the information that can be exchanged and to its possible uses should be recalled here.
[221] Importantly, similar limitations may not be in place at the domestic level, in the context of ordinary cooperation and coordination between the FIU and other national agencies (for example, through dissemination and exchange of information).

(both domestically and internationally). Nonetheless, in the current state of affairs, due to uncertain or inadequate legal bases, it seems that the potential of diagonal cooperation for FIUs to uncover criminal or anomalous activities related, but additional, to money laundering or terrorist financing remains significantly unexploited and these forms of international cooperation are substantially under-utilised.

Existing differences in the forms and modalities through which diagonal cooperation is carried out by the FIUs that have the capacity to do so represent another significant obstacle to the development of the exchange of information with foreign non-counterparts.

As seen in previous paragraphs, while several FIUs can only provide information diagonally through indirect transmission to the FIU of the country concerned, a significant number of them can instead liaise directly with foreign non-counterparts, which raises the issue of lack of communication with the FIU of the country concerned. This is particularly important when STR/SAR information is transmitted. Even in cases of indirect diagonal cooperation, there seems to be no indication on whether the information should be passed on to the final recipient through the local FIU (as is now customary, given that indirect diagonal cooperation is carried out based upon the general provisions and procedures about FIU-to-FIU cooperation) or through other authorities, domestic or foreign (as allowed by international standards: see paragraph 1).

These differences carry a significant potential to further limit diagonal cooperation as the information may be exchanged to a different extent or through different channels or procedures by the parties involved, raising for example problems of reciprocity or data protection (related to, i.a., possible prohibitions to communicate STR/SAR information to foreign agencies).

Also due to the different forms and procedures used for diagonal cooperation, an issue of security and adequate protection of STR/SAR information has to be flagged. Whilst the fourth Directive requires that appropriate protection is ensured to the information exchanged, particularly through the use of dedicated secure channels (see article …), outside of the FIU-to-FIU communication networks there are not guarantees that appropriate and commensurate safeguards are applied to the circulation of STR/SAR information. As diagonal cooperation can be carried out by means of direct communication with foreign non-FIU counterparts or through agencies that are not FIUs, risks of inadequate data secrecy and protection in the transmission also play a significant role as a deterrent to diagonal cooperation.

Another potential problem area for consideration is the lack of involvement of the FIUs of the countries concerned in cases of direct diagonal exchanges where FIUs send information to non-FIU foreign authorities and do not inform their local counterparts. This issue becomes particularly relevant when the diagonal exchange is related to STR/SAR information or otherwise to suspicious money laundering or terrorist financing cases on which the local FIU may have inputs to provide or may be interested in carrying out own analyses.

As highlighted in previous paragraphs, cases of direct transmission of information to foreign non-FIU counterparts are currently reported by police FIUs which exchange information with law enforcement agencies in other countries, specifically through the police international cooperation mechanisms. To the extent that the information exchanged derives from STR/SAR or concern suspicious money laundering or terrorist financing activities, the question arises of whether in these cases the exchange should be carried out in the context of the FIU-to-FIU cooperation, rather than through law enforcement cooperation channels. There is also a risk that, as also discussed in relation to the FIUs' analysis function and cooperation, the necessary distinction between FIUs'

activities and cooperation and law enforcement activities becomes blurred, with the former being absorbed into the latter.

To establish a robust framework underpinning FIUs' diagonal cooperation and address the issues outlined above, the setting up of a uniform legal framework at the EU level on some key points, in line with FATF and Egmont standards on the same matters, appears necessary.

- There should be a requirement for Member States to empower FIUs to exchange information (either by requesting it or providing it in response to others' requests) with non-FIU counterparts from other Member States for appropriate purposes. These should include, in addition to preventing and detecting money laundering, predicate offences and terrorist financing through intelligence, the support to law enforcement activities, fiscal controls, supervisory actions (thus enlarging the current "purpose limitation").

- In line with international standards, diagonal information sharing between FIUs and other "eligible" foreign agencies should be possible but not mandatory, contrary to the FIU-to-FIU exchange which, according to FATF standards and EU provisions, are due in all cases and cannot be refused.

- Also to compensate for the wider scope of international information sharing resulting from the derogation to the "purpose limitation", conditions limiting the exchange could be applied, such as those about reciprocity (foreign non-FIU agencies should in turn be able to send information to FIUs upon their requests). For the same reasons, obligations of adequate use and protection of the STR/SAR information shared should also be required.

- Appropriate and uniform modalities and channels should be set out for carrying out diagonal cooperation under a regime common to all EU FIUs. In this context, the use of secure communication channels for the transmission of STR/SAR information, typically those in use for the FIU-to-FIU cooperation, should be required.

- With a view to allowing for secure communication channels and ensuring that all interested FIUs are appraised and duly informed about diagonal exchanges concerning potential money laundering or terrorist financing cases relevant to their countries, diagonal exchanges should take place indirectly, through the FIUs of the countries involved. In case of direct diagonal sharing, should these be allowed, while requiring that FIU-to-FIU cooperation mechanisms are not replaced by law enforcement channels, there should be a requirement to inform in all cases the FIUs of the countries concerned.

CHAPTER 8

DATA PROTECTION, CONFIDENTIALITY, SECURITY

1. Introduction

Data protection, confidentiality and security issues play a critical role in the activities of a financial intelligence unit. Appropriate confidentiality and security requirements are essential for the proper and effective functioning of FIUs, in particular in two separate but complementary aspects:

- At the domestic level, it is necessary to ensure that sensitive STR/SAR information is duly protected to both safeguard the reporting entities and not to affect possible investigations or prosecutions;
- In the context of FIU-to-FIU cooperation, the existence of adequate and uniform confidentiality and security guarantees is essential to give FIUs the confidence that is needed to allow the sharing of sensitive information.

Information confidentiality and security issues are considered an intangible element of international standards on what constitutes a FIU and are present in publications of international organizations, such as the FATF and the Egmont Group[222]

The topic of data protection, information security and confidentiality is incorporated into FATF Recommendation 29 regarding financial intelligence units. The interpretive note to R29 explicitly states, that "information received, processed, held or disseminated by the FIU must be securely protected, exchanged and used only in accordance with agreed procedures, policies and applicable laws and regulations". In order to be compliant with this section of R29, the FIU should protect information by:

- having rules in place governing the security and confidentiality of information, including procedures for handling, storage, dissemination, and protection of, and access to, information;
- ensuring that FIU staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information;
- ensuring that there is limited access to its facilities and information, including information technology systems.

The aspects of FIU information security and confidentiality are not explicitly covered by the provisions relating to the FIU in the fourth AML/CFT Directive. However, two recitals of the fourth Directive refer to data protection and security aspects associated with the role of obliged entities in

[222] *„Securing an FIU – Operational Guidance*"

the AML/CFT system. Recital 41 refers to the necessity of Member States to guarantee the confidentiality of the identity of employees reporting suspicions of money laundering to the FIU, in order to protect them from threats or hostile action. The domestic AML/CFT system can only function when private sector staff is confident, that they can provide information on possible suspicious activity to the FIU without putting themselves at risk. Recital 43 highlights the necessity for Member States to implement the fourth Directive in full alignment with the existing EU law, especially the Union data protection law and the protection of fundamental rights as enshrined in the Charter. Data gathered, analysed, stored and shared due to the provisions of the Directive should be processed only for the purposes and activities stated in the Directive. The collection and subsequent processing of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of the Directive and personal data should not be further processed for other reasons – especially commercial purposes.

Both international standards and the fourth Directive relate to different aspects of data protection, confidentiality and security issues. Based on the responses to the survey, it seems that EU FIUs consider themselves in line with these standards. Data Protection, confidentiality and security is considered as an issue of upmost importance by all financial intelligence units. This reflects the number of additional comments provided by the respondents to questions regarding this topic. EU FIUs have provided in their responses information on various procedures and solutions responsible for ensuring data security and confidentiality. For the purposes of this report, measures concerning data protection, confidentiality and security issues have been divided into two categories:

- Confidentiality and security safeguards throughout the FIU's operational and analytical work cycle;
- Confidentiality and security safeguards at the organisational level (staff, equipment, premises, clearance levels, procedures, etc.).

The rules governing these both aspects of FIU information security and confidentiality are set out in the legal framework of each member state.

2. Legal framework on confidentiality and security

EU FIUs have introduced a variety of safeguards to ensure data protection, security and confidentiality throughout the FIU work cycle. These safeguards are introduced into the domestic AML/CFT frameworks by appropriate rules incorporated in legal acts and internal regulations. All FIUs, which have responded to the questionnaire signalled, that they consider themselves to have appropriate rules for managing the security and confidentiality of the information received, stored processed and disseminated by the FIU.

Several FIUs provided additional insights as to the legal framework associated with these rules. In general, all respondents indicated, that rules concerning information security and confidentiality are not restricted to provisions of one single legal act. They can be located within several documents, such as:

- the domestic AML/CFT Act;
- general acts regarding data protection;
- internal regulations of host institutions, in which the FIU is embedded;
- internal procedures of the FIU concerning the handling of information;
- guidance and instructions concerning information security;
- international regulations (i.e. protection of data exchanged).

A first glance at information provided by EU FIUs regarding information security and confidentiality reveals significant differences in the variety of safeguards applied and how these safeguards are regulated by Member States. The absence of provisions concerning security and confidentiality in the Directive and previous EU legislation allows national governments to structure the scope and content of data protection, security and confidentiality rules. While responses do not indicate directly any challenges associated with the different approach of EU FIUs, the lack of a common approach leads to situation, where different levels of information security and confidentiality can be applied in various Member States. These differences may have a direct influence on FIU functions in two spheres: the domestic sphere – the willingness or obliged entities and competent authorities to provide information to the FIU - and the international sphere – the willingness of foreign counterparts to engage in information exchange with the aforementioned unit.

3. Confidentiality and security requirements in the FIUs' functions

Respondents to the survey have indicated different aspects of data protection, security and confidentiality, connected with particular tasks conducted by the FIU. For the purposes of this report, emphasis has been put on the core activities of financial intelligence units integrated in the FIU work cycle. The following aspects of this work cycle will be highlighted:

- the receipt of data;
- the handling of data;
- access to external sources of information;
- domestic dissemination of intelligence products;
- FIU-to-FIU exchanges.

3.1. The receipt of data

EU FIUs have a variety of different solutions in place regarding the receipt of information from reporting entities and competent authorities. Differences concerning the data sources available to the FIU and the information content have already been analysed in chapters 3 and 4 of this report. These elements are interconnected with safeguards ensuring the security and confidentiality of the received information.

Secure information channels is an aspect highlighted by many FIUs when referring to data protection associated with the receipt of data. As underlined in chapter 3, the majority of disclosures containing STR/SARs and threshold based reports are conducted with the use of electronic channels. FIUs have established various procedures allowing to receive such disclosures, such as dedicated web based -reporting systems, encrypted files and secure emails. These channels provide sufficient security measures, allowing the FIUs to register the data transfer and access to these disclosures.

Some FIUs have also highlighted, that many disclosures are still provided in a paper-based format.

> A respondent has informed that "STRs are received by mail, E-file (a secure channel provided by Fundsquare) and OTX (a secure channel provided by the national IT services center called "CTIE"); sending the reports encrypted by e-mail is discouraged".

These disclosures can be delivered to the FIU either in registered mail or using courier services. It seems however, that aforementioned methods are being phased out due to the time consuming

process of integrating the received information with the internal databases of the FIU. Although this channel cannot be subject to cybercrime, it is in most cases dependant on courier or postal services which raise the risk of the information being intercepted.

"The main reporters use a bulk data transfer mechanism which is more appropriate for their volumes. For this, the [FIU] provides 'Public Key Infrastructure' encryption certificates which allow high volume reporters to submit encrypted files directly onto the SARs database. Most other reporters use SAR Online, a secure web-based reporting mechanism that, upon registering, can be used by anyone with internet access. A very small number of SARs are still submitted on paper".

3.2. The handling of data

The handling of data constitutes a wide array of activities from data storage, processing to archiving. These aspects are connected with safeguards at the organisational level, especially those regarding the existence of dedicated IT systems and access to FIU premises where information is available. FIUs in their responses regarding this aspect have described the existence of backup procedures and encryption procedures ensuring necessary data security.

As put by a respondent, "the current handling of STRs through electronic systems, whose access is limited to the personnel in charge of analysis, has increased the level of security, thus providing for limited access through procedures of authorization granted on the basis of the functions performed, as well as of authentication. Databases protection from unauthorised access is also in place, as well as specific backup procedures, in order to guarantee the recovery data, as well as encryption procedure on the transmission and memorization of data. The FIU has put in place a wide range of technological means, (i.e., security software, hardware) to keep information and facilities secure".

More information concerning safeguards connected with dedicated IT systems will be enclosed in the section regarding information and security safeguards at the organizational level.

3.3. Procedures for the access to external sources of information

An analysis of EU FIUs' powers regarding the possibility to access external sources of information, such as law enforcement, financial and administrative information, conducted in chapter 3 of this report, has identified various solutions used by FIUs to obtain the necessary data. In general these solutions can be related to direct and indirect access to external sources.

Direct access by the FIU to external data sources offers many advantages. Apart from aspects related to quick response times and easier integration into FIU IT systems, these solutions also provide additional safeguards regarding information security and confidentiality. One of these safeguards is the possibility of the FIU to protect information regarding the content of queries it conducts. In the case of external databases managed by other national authorities, several FIUs can question the system directly, without the need to contact the staff of these institutions. In cases requiring personnel to process the requests, obliged entities often possess dedicated staff, which are subject to additional internal confidentiality and security requirements. These measures allow FIUs using direct access to external sources to provide higher levels of data protection than indirect access.

Indirect access, either through a decentralized retrieval system or via a third party, possesses more vulnerabilities from the information security and confidentiality perspective. The addition of an additional step in the process of obtaining information - an intermediary – is a factor which has to be taken into account when considering data protection. The existence of such an intermediary

raises the risk of information on requests and responses being misused without the knowledge of the FIU. On the other hand, some FIUs use liaison officers allocated in their unit, to govern the process of obtaining information from external sources. This solution significantly limits the risks associated with indirect access to these sources.

3.4. Domestic dissemination of intelligence products

EU FIUs in their responses to the survey have provided different remarks concerning procedures covering secure dissemination of information. Similarly as in the case of receiving information from reporting entities and competent authorities, FIUs highlighted the role of secured channels of communication to guarantee information security and confidentiality. One financial intelligence unit has informed, that it gives accredited LEA staff members access via an electronic system to such reports (in a sanitized version). Access to suspicious activity reports is granted on the basis of relevant end-user agreements that must be signed by the end-user agency and the individual end-user who has access to the material.

"The database stores all SARs submitted by the reporting sector. It is owned and managed by the FIU. The database is managed in an appropriate way so as to allow accessible information for use by SARs regime stakeholders, where appropriate. Direct access to the database is restricted to FIU officers. Instead of disseminating SARs to end users, the FIU makes a restricted version of the database available through a portal called money.web. Information of a particularly sensitive nature is removed and there is a seven day delay between a SAR being received and it being available for view. These seven days allows sensitive material to be removed by the FIU. Access is limited to accredited financial investigators (FIs), financial intelligence officers (FIOs), a recognised equivalent, or those that have completed other approved accreditation to the same standard".

Other FIUs have also provided insights on the procedures and solutions regarding the dissemination of intelligence products to competent authorities.

On this note, for example, "the FIU forwards documents to the direction of the investigative authority and the police (as dissemination) electronically in a secured and protected electronic network. In all other cases the FIU staff forwards the documents to the consignee personally and directly. The transportation of the documents is done with using office cars, which are exclusively used by the FIU members".

Another respondent points out that "In order to strengthen exchanges with the investigative bodies, increasing further efficiency and timeliness, FIU created a new internet channel, dedicated to the exchange of information with the investigative bodies. Through the portal, reports and related technical reports are forwarded to the Law Enforcement Bodies in real time. The Law Enforcement Bodies therefore receive reports, classified according to the final rating assigned by FIU and enriched by all the evidence gathered during the first and second level analysis".

3.5. FIU-to-FIU exchanges

International information exchange is a function particularly sensitive to data protection, and confidentiality issues, as security measures have to be agreed upon by all parties involved. In order to facilitate such exchange, both the EU and the Egmont Group have dedicated resources to the construction of dedicated channels for international cooperation between FIUs. The fourth Directive refers to the necessity of FIUs to use protected channels of communication. Article 56(1) explicitly

encourages also EU financial intelligence units to use FIU.NET (or, in the future, its possible successor) as the appropriate secure channel for information exchange between Member States.

Unsurprisingly, FIUs in their information exchange rely on existing dedicated communication channels developed by the European Union and the Egmont Group. Three FIUs have mentioned in their replies the procedures regarding international information exchange, focused on the use of FIU.NET and the Egmont Secure Website. Two of these FIUs have stated that information received internationally is protected by the same safeguards as information received from domestic sources.

One of the aforementioned units has also directly referred to the fact that its procedures regarding data security in the context of international cooperation are in line with the FIU.NET Users Protocol and Egmont Group best practices published in the report on *Securing an FIU – Operational Guidance*.

"The FIU uses ESW or FIU.NET for its international communications concerning STR information. This, besides ensuring security and confidentiality, allows identifying univocally and clearly the channels and gateways to be used for international cooperation. The access to and the use of ESW and FIU.NET are strictly limited and regulated and appropriately secured by internal rules of procedure. In accordance with FIU.NET Users' Protocol and Egmont Group's best practices, only authorised personnel may have access to such gateways".

The FIU in question has also highlighted, that on rare occasions, there may be a need to use other communication channels apart from FIU.NET and ESW, for example when exchanging data with a non-Egmont FIU.

4. Confidentiality and security safeguards at the organisational level

Apart from putting in place various procedures governing data protection, confidentiality and security in the work – cycle, FIUs have also introduced a series of measures at the organizational level aimed at ensuring information security and confidentiality. These measures can be divided into three key spheres regarding: FIU facilities, IT systems and staff.

4.1 Access to FIUs' facilities and protection of information security

Nearly all FIUs have indicated that they have limited physical access to their facilities. Twelve of the respondents noted, that there is limited access to the FIU premises. Taking into account the answers provided, it seems that European financial intelligence units use a variety of measures to secure limited access to their quarters. Respondents have in particular touched upon two key elements regarding this area: special areas with restricted access and other physical barriers preventing unauthorized access.

Special areas with restricted access: Six financial intelligence units described the existence of special facilities within the FIU premises, where classified data may be stored or processed. Access to these areas is restricted to particular staff members. One respondent mentioned "*a separate room where confidential data is processed".* Another FIU indicated the existence of "*secure facilities for storing data, both in hard copy and electronic form*". One unit provided information on "*the server room, which is restricted to authorized personnel only*". Another FIU pointed out, that it restricts access to data centres, in which information is stored.

Other physical barriers preventing unauthorized access: One FIU mentioned, that "*the premises are equipped with intruder alarms, CCTVs and other technological and IT measures aimed at securing*

and monitoring entry to the FIU quarters". Another respondent to the survey indicated, that its offices are secured by burglar alarms, fire alarms and cameras. Two Financial Intelligence Units have informed that their premises are physically protected by guards or a police formation. Another two units informed about employing staff, which are dedicated to security matters. Two respondents mentioned restrictions concerning visitors to FIU premises. One of these FIUs has informed that visitors in the office have to be accompanied by its staff.

"The premises are under constant CCTV surveillance and access to certain sensitive areas, such as the server room, is restricted to authorized personnel only". Moreover, as pointed by the same respondent, "all the workstations of the officers of the FIU are secured by a password and access to the databases is subject to logging system which keeps a trail of all the activities conducted by each authorized member of staff".

4.2. Restricted access to IT systems managed by the FIU:

EU FIUs regards the use of sophisticated in house IT systems as one of the key elements of their safeguards guaranteeing information security and confidentiality. More than half of respondents explicitly highlighted in their descriptive comments, that they have secured restricted access to their IT systems, containing information possessed by the FIU. At least ten of these units clearly stated, that there is no possibility to externally access their IT systems and databases – this is limited to FIU staff. Only in two cases FIUs have signalled, that representatives of other authorities have the possibility to directly inquire IT systems managed by the FIU or access information contained in these systems. At least one FIU mentioned that it possesses its own internal IT staff to maintain the infrastructure. Two FIUs have mentioned an important feature of their IT systems, allowing for each activity conducted to be registered and monitored. Many FIUs have indicated that a dedicated password (and in one case also an identification badge) is necessary to access the IT systems of the FIU.

5. Security clearance levels for staff and understanding of responsibilities in handling and disseminating the information

All EU FIUs are confident, that their personnel possesses the necessary security clearance levels and understands the responsibility connected with the handling of sensitive and confidential data. FIU comments concerning information security and confidentiality measures associated with staff can be categorized into four different categories: security clearance, employee screening, the responsibilities of FIU staff in reference to confidential data and training and awareness raising activities.

5.1 Security clearance for staff members

Several FIUs have explicitly mentioned in their comments, that their staff possesses various levels of security clearances. The respondents have also provided information on different minimum levels of security clearances possessed by their staff. One FIU noted generally, that its staff has authorized access to EU confidential documents. Another FIU pointed out, that the lowest access level is restricted. In two cases, all STRs received by the FIU are treated as classified information. Additional comments provided by the respondents also indicates that staff members have different levels of security clearance within one organisation. Replies suggest that the level of access to classified documents can be dependant either on the position of the employee (his rank in the structure) or due to the field, in which he operates. Some FIUs indicated particular types of job positions, which require high level of access to classified documents. Another FIU explained, that staff dedicated to terrorist financing issues has a higher clearance level, due to their need to

cooperate with competent authorities in this area. Two respondents explicitly pointed out, that security clearances are provided to FIU staff strictly on a need to know basis. Some FIUs highlighted, that part of their personnel also has clearance for EU and NATO classified documents.

Replies regarding security clearance for personnel and procedures concerning the handling of information by FIUs indicate that financial intelligence units may classify their information on different levels of security clearance. The tendency to assign high classification levels may hinder possible information exchange with foreign counterparts.

5.2 Screening of employees and recruits

Many FIUs have highlighted that their employees are subject to security screening either when they are recruited for positions within the unit or throughout the course their employment. At least three FIUs conduct screening during the recruitment process. Respondents have indicated the use of both an internal and external screening processes. In one case, the FIU has noted, that the person involved cannot commence his work until the screening is complete. Another unit has highlighted that its recruits are screened by the security services before being hired. Apart from the initial screening during recruitment, some FIUs conduct screening processes periodically. Others conduct them when employees apply for a higher clearance level regarding classified documents.

For example, a respondent has explained that "all FIU employees undergo security screenings that establish if the person is suitable for work of importance for the security of the nation and of significant anti-terrorism importance. The person cannot commence work in such sectors until the screening is complete. Security screenings are subsequently performed repeatedly".

In another case, "the National Police Act as well as other specific laws governing national security stipulate that for certain government positions (such as FIU staff) the National Police can perform security clearance screening on personnel and new staff before hiring in order to make sure that proper security clearance can be given".

5.3 The responsibility of the FIU personnel to safeguard information

Several respondents have highlighted in their comments to the questions in this section the responsibility financial intelligence unit staff to maintain the confidentiality of information within the possession of the FIU.

Some FIUs specifically underlined, that their employees are obliged to not disclose information or facts that they have become aware of during the performance of their job. One respondent explicitly pointed out, that this obligation is also valid after the staff member leaves the FIU. At least two FIUs have informed that their personnel is required to sign an agreement or declaration which prohibits them from disclosing any information received during their employment with the FIU. One of these FIUs has stated that if the personnel involved infringes any of their legal obligations they incur civil, criminal or disciplinary liability. Another FIU has also indicated that the failure of staff members to fulfil requirements concerning the confidentiality of information in the possession of the unit is punishable by criminal sanctions.

"In addition to the classification system of FIU information, Article 25 of the AML/CFT Law prohibits the personnel of the FIU from disseminating information received in the performance of their functions. The information received may not be used for the personal interests of the personnel of the FIU, either during or after their employment. According to the FIU Regulation, at the start of their employment, the personnel of the FIU is required to sign an agreement which

prohibits them from disclosing any information received during their employment with the FIU, except in the case of a judicial procedure. According to the FIU Regulation provides that where the personnel of the FIU infringe any of their legal obligations they incur civil, criminal or disciplinary liability, as the case may be, according to the law".

5.4 Training and awareness raising activities

Many respondents have highlighted methods of ensuring that FIU staff members endorse information security and confidentiality policies. In at least two cases, employees are introduced to these regulations upon recruitment to the Unit. One FIU has mentioned that new employees undergo special training on security and confidentiality. Another respondent has highlighted that staff members are required to take an exam regarding confidentiality policies. This FIU has also informed that those who seek access to SARs must first complete a SARs confidentiality training course.

For example: "The FIU has internal policies and operating procedures in place for all staff, giving a detailed overview of the SARs Regime, describing the component parts of the FIU and further reinforcing with staff the criteria for access to, and constraints on, the use of SARs material. All FIU officers – and NCA officers – who seek access to SARs material must complete a 'SARs confidentiality' training course based on NCA policy and the Home Office Circular on the confidentiality and sensitivity of SARs and the identity of those who make them. This describes the duty of care to reporters, the general outline of the FIU and how material from SARs can be used. FIU officers are also either financial intelligence officer or financial intelligence administrator accredited. Both require completion of training courses and exams relating to SAR confidentiality, plus provide ongoing support by way of continued professional development in order to share best practice and provide assistance in the correct way to use SARs material".

6. Conclusions

The responses to the survey suggest that EU Financial Intelligence Units are in line with international standards concerning data protection, confidentiality and security, incorporated within FATF Recommendation 29. FIUs have rules in place governing the security and confidentiality of information and procedures for handling, storage, dissemination, protection of, and access to, information. Respondents indicate that FIU staff members have the necessary security clearance levels and understanding of their responsibilities in handling and disseminating sensitive and confidential information. All FIUs also informed that there is limited access to their facilities and information, including information technology systems.

Information security and confidentiality is an area to which FIUs have always devoted a considerable amount of attention. Nevertheless, it is apparent that the requirements provided in the interpretative note to Recommendation 29 regarding information security and confidentiality are very general. A close look at the various responses and different solutions provided by EU FIUs reflects the differences in the size, nature and status of EU FIUs, local circumstances and the particular national "mix" of competences distributed across different AML/CFT authorities and bodies.

Taking into account information provided by Financial Intelligence Units regarding data protection, security and safeguards at the organizational level, it seems that Member States and EU FIUs have put in place strong and comprehensive measures in line with FATF standards in this area. FIUs have referred to various solutions, in particular limiting access to FIU premises, IT systems and data along with safeguards associated with personnel.

Nevertheless, an analysis of information security and confidentiality safeguards regarding the FIU work cycle reveals significant differences in how information is received, obtained, processed or otherwise handled while performing the FIUs' core functions and how it can be shared or communicated, either within the FIU, with domestic third parties or with foreign counterparts. Based on responses, this "legal" aspect seems to be less uniform and less regulated across the EU than the aforementioned organizational safeguards. EU FIUs are subject to differing confidentiality regimes, based on domestic legislations, determining how the information should be processed and kept confidential in the exercise of their core functions.

It is important to underline, that differences in data protection, security and confidentiality measures maintained by EU FIUs can have a negative influence on the capacity of these units to exchange information with each other. An analysis of FIUs' power to exchange information conducted in chapter 6 suggests that data protection limitations lie also at the basis of restrictions which prevent some FIUs from accessing and sharing specific categories of information. Additionally replies concerning the handling of information by FIUs indicate that Financial Intelligence Units may classify their information on different levels of security clearance. The tendency to assign various classification levels may create obstacles possible information exchange with foreign counterparts.

Uneven safeguards across Member States and FIUs on how information is treated is a factor that can greatly discourage cooperation and the sharing of information. In order to address this issue, a more robust, comprehensive and uniform legal basis at the EU level regarding data protection, security and confidentiality safeguards may need to be considered. Such provisions setting out appropriate minimum safeguards could be focused on the core functions composing the FIU work cycle: receipt, analysis (handling of data), access to external sources of information, dissemination and exchanges with other FIUs (including diagonal).

CHAPTER 9

MOST RELEVANT PROBLEMS OR SHORTCOMINGS ENCOUNTERED IN FIU-TO-FIU COOPERATION

1. Introduction

The survey on shortcomings that affect EU FIUs' activities, powers and cooperation, has been conducted in the previous chapters on the basis of information provided by respondents on discrete, pre-identified issues and on the analysis conducted on such information. Under this "bottom up" approach, the survey attempts to identify existing problems and their root causes by mapping FIUs' features and activities, comparing them with what is required by relevant EU provisions and international standards and elaborate on the adequacy and effectiveness of FIUs' action in key areas.

This analysis is complemented, in this Chapter, by an overview of inputs and comments provided by EU FIUs on the most prominent problem areas where they experience difficulties in conducting effective cooperation activities and where they think that improvements should be realised in the EU framework. The problems mentioned and the comments provided by FIUs, based on their direct operational experience, match significantly the findings emerging from the analysis conducted.

In fact, in line with the findings recalled in previous Chapters, EU FIUs have consistently referred to, as the most relevant obstacles that still limit the effectiveness of cooperation within the EU, issues related to, i.a.: differences in FIUs' status and powers; refusals based on the need for prior STRs/SARs or to existence of investigations or to the need to use law enforcement cooperation channels; lack of cooperation due the identification and type of underlying offences; insufficient capacity to obtain and share information; insufficient capacity to provide consent for further use or dissemination of the information exchanged.

These issues, as emerging from FIUs' responses to the survey, are succinctly outlined in the following paragraphs.

2. Difficulties deriving from differences in FIUs' status and powers

Several respondents have indicated that FIU-to-FIU cooperation is significantly affected by existing differences in national AML/CFT regimes and in EU FIUs' status (specifically as regards their organizational nature and setting) and the powers available. This clearly indicates that FIUs firmly believe that domestic regimes and arrangements heavily influence the capacity to provide cooperation, as the former determines the scope of information available and of powers exercisable to sustain the latter.

Across the considerable range of issues raised by respondents, the following emerge more prominently from the survey (some of the elements submitted will also be touched upon further down, under different topics):

- general differences in national AML/CFT legislations which hinder the FIUs' capacity to engage in cooperation with foreign counterparts; relevant aspects include the definition of "money laundering", the scope and nature of its predicate offences, the definition of "terrorist financing", data protection and confidentiality safeguards;
- differences in national disclosure regimes (e.g. SAR versus STR), implying that FIUs receive different information, which reflects on both the nature of their activities and the capacity to provide cooperation;
- differences in FIUs' powers and in national provisions governing the exchange of information;
- FIUs' access (or lack of it) to data, particularly as regards the differences between administrative FIUs and police/judicial FIUs;
- specific problems and limitations in obtaining and sharing banking information;
- the need that requests meet domestic thresholds on necessity and proportionality.

A respondent, for example, has explicitly indicated that "the differences between administrative FIUs and police/judicial FIUs' responses must decrease" to allow for more effective cooperation. Another respondent has stated that, whereas some FIUs share extensive information (financial, criminal, administrative), others only share small amounts of information which only minimally benefits investigations.

3. Need for a prior STR/SAR as a condition to provide cooperation

Some respondents recall that one major obstacles in receiving cooperation from other EU FIUs lies in the condition to which some of those are subject that prior STRs/SARs be received on the same case or subjects involved in the request. These are cases where, the requested FIU can only provide information available or exercise its powers to obtain information on behalf of foreign counterparts if relevant STRs/SARs have already been received.

In particular, those respondents report that sometimes "the requested FIU objects that it lacks the power to act upon a case which has not been already reported as suspicious in its own country, thus preventing it from collecting and sharing information."

4. Refusal of cooperation due to the mere existence of investigations or legal proceedings

Respondents point out that in several cases FIUs improperly deny cooperation for analytical purposes on the sole ground that investigations or legal proceedings are underway in their countries on the same cases or on the same subjects involved in them. Importantly, these are cases where the cooperation is refused for the mere existence of investigations or legal proceedings regardless of the potential impact of the cooperation requested on such investigations or proceedings.

These cases of denial are often associated with a broader underlying issue, also highlighted by respondents, that is the lack of capacity for some FIUs to provide information directly and the need, to obtain this information, to make use of separate mutual legal assistance channels (see the following paragraph).

5. Refusal of cooperation due to the need to use law enforcement channels

Respondents report that "FIUs may improperly deny cooperation for analytical purposes on the ground that the issue should be dealt with through mutual legal assistance channels". This can be the case "despite the existence of STRs and the need to develop a separate and autonomous financial analysis within the interested FIUs."

A respondent highlights that obtaining information on bank account is in some cases impossible through FIU-to-FIU cooperation and remarks that "EU FIUs should be encouraged to exchange information on bank accounts directly as intelligence with their FIU counterparts, instead of indicating that this information should be required through MLA channels".

Another FIU has stated that police-type FIUs do not provide financial information, referring the requesting (usually administrative-type) FIU to the MLA channels of cooperation; the same respondent note that, "however, the requesting unit cannot use this way to obtain the required information as the conducted analysis (investigation) has a character of intelligence, not criminal proceeding".

6. Refusal of cooperation due the identification and type of predicate offences

Several respondents highlighted the problems and shortcomings associated with the requirement to set out, in the request, the predicate offence underlying the 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. Respondents 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.

A respondent emphasizes that in many cases requests for cooperation are declined on the grounds of the "lack of indications about the predicate offence which may be underlying the case under analysis or differences between predicate offences in the countries involved. These are cases where the existence of a predicate offence and the type thereof, which is certainly not something which is supposed to emerge clearly in the analytical stage at which FIUs operate, has an effect upon the administrative cooperation."

Another respondent points out that conditions and limitations related to the identification and nature of predicate offences are often applied at the stage of the prior consent, requested for further using or disseminating the information exchanged (see also, on this, paragraph 8 in this Chapter and paragraph 10 in Chapter 6): there are "difficulties and shortcomings when it comes to providing the consent to further use or dissemination, after the initial exchange of the information for the FIU's own analytical process. In such events, it is still frequently the case that such consent is denied because of the nature of the predicate offence which is assumed is underlying the case or, even worse, simply because no specific predicate crime can be identified by the FIU seeking the consent".

In this context, the issue of tax crimes has been particularly underscored: difficulties have in fact been reported in obtaining "information tied to taxes" because some FIUs, based on their domestic laws, "do not consider tax offences as predicate offences for money laundering".

On the difficulties in providing adequate FIU-to-FIU cooperation associated with the (lack of) description of the underlying criminality and the nature thereof, see also the considerations in paragraph 9 in this Chapter, on existing expectations and domestic requirements that requests are substantiated also through an adequate description of the offences at stake.

7. Lack of capacity to obtain or share information

One the most significant and shared concerns about the FIUs' capacity to provide effective cooperation pertains to the shortcomings that continue to limit FIUs' ability to obtain information domestically and exchange that information with foreign counterparts. In this perspective, respondents repeatedly flag issues distinctly related to:

- the insufficient range of information that in many cases can be provided in response to requests for information;
- the diverse scope of powers and capabilities across EU FIUs in obtaining and sharing particular types of information (so that the same types of requests are often responded differently by different counterparts).

For example, a respondent has stated that "whereas some FIUs share extensive information (financial, criminal, administrative), others only share small scale of information. In these cases the information minimally benefits investigations". A respondent also flags the "inconsistency with levels of information provided" by EU counterparts, whilst another emphasizes that many FIUs never made it clear which information they could share", thus making the exchange particularly uncertain.

Insufficient capacity to obtain and share information is found to be particularly significant in relation to certain types of data, notably banking information. More in general, respondents flag that poor FIUs' capacity to share information is in many cases a consequence of the insufficient capacity to obtain or access the information needed to respond to requests by making use of their domestic powers and availing themselves of relevant databases.

7.1 Lack of banking information

Some respondents point out that it is sometimes "hard to get the banking information needed for the analysis from the other FIU". One of these respondents states that, on the contrary, it itself includes in responses "the transactions history (trace of the money) and data regarding the bank account owners". This is echoed by another FIU that clarifies that "we always provide information from our national bank account registry or on the contents of requested bank accounts even in cases of non-reciprocity".

One FIU has remarked that "EU FIUs should be encouraged to exchange information on bank accounts directly as intelligence with their FIU counterparts, instead of indicating that this information should be required through MLA channels". Another respondent recalls that some FIUs only share banking information if this information is connected with an already received STR (see also paragraph 3 on this last point).

Existing limitations to the access to information concerning holders of bank accounts, particularly due to the lack of dedicated centralised national databases, are specifically mentioned by respondents. Four FIUs states that "not all countries have a national banking and payments accounts register, therefore in some cases it is difficult to identify subject's bank accounts, held in foreign countries". One respondent indicates that this "lack of reciprocity … as regards the information that

can be shared, [i.e. in that] some FIUs still do not have access to bank accounts holders nor can obtain banking and financial information" was a "very relevant shortcoming" (this respondent acknowledges that the problem should disappear following the implementation of the fourth Directive).

7.2 Insufficient capacity to obtain information and access databases

Several responses to the survey flag problems surrounding the FIUs' capacity to access relevant data sources with the aim of sharing information with foreign counterparts. These problems are mentioned specifically in relation to the insufficient availability of law enforcement information: some respondents highlight on this point that FIUs are subject to significantly different regimes in their own countries for accessing and sharing police information, with uneven results as to their capacity to obtain and share this information to a sufficient extent with foreign counterparts.

Deficiencies are also mentioned in the capacity of EU FIUs' to access and exchange tax-related information.

Other respondents referred to the difference between the FIU's powers to access information on tax matters and to the related difficulties in getting complete answers due to the insufficient databases available to foreign counterparts approached.

One respondent has added that it is in many cases unclear, on an "ex ante" basis, which possible databases an FIU can search to obtain information in response to foreign requests.

7.3 Insufficient capacity to obtain information from obliged entities

Some respondents have also highlighted that several EU FIUs still do not have sufficient powers to obtain information from obliged entities, for domestic analysis and particularly for FIU-to-FIU cooperation, in accordance with the FATF standards and the fourth Directive.

A respondent has emphasized more specifically that the combined effects of the lack of power to obtain information from obliged entities on behalf of foreign FIUs and the condition that cooperation can only be provided if an STR/SAR has already been received on the same case (both present in conjunction for some FIUs) often result in the complete incapacity to respond to requests for information.

8. Insufficient capacity to provide the consent for further use or dissemination of the information exchanged

A significant number of respondents flag existing obstacles that prevent FIUs from further using the information received, particularly through dissemination to domestic competent law enforcement agencies for the appropriate follow up to the analysis, due to the delay or outright refusal in giving the necessary prior consent by the providing FIU. These obstacles are related to both the prolonged timeframe needed to obtain feedback on requests for further use or dissemination of the information exchanged and the frequent cases where the consent for such use or dissemination is denied, with negative impacts on the effectiveness of the ensuing law enforcement action.

Specifically on the timeliness issue, a respondent emphasizes that the initial feedback received from foreign FIUs often does not include the consent to forward the information obtained to relevant law enforcement agencies, as requested to ensure the appropriate follow up to the analysis; such consent then has to be asked for specifically, which may cause delays in following up on the case.

The issue of the timeframe has been raised by another respondent, who has stated that the obstacles encountered in receiving sufficiently quick responses to requests for consent may make it impossible to issue a timely order to reporting entities to temporarily suspend the execution of suspicious transactions. It is suggested to speed up the information exchange between EU FIUs, including as regards the release of the consent for dissemination of the information as intelligence to competent authorities.

Respondents bring forward some suggestions on possible ways to address the difficulties associated with the excessively long timeframe for obtaining the consent.

For example, it is proposed that, to make FIUs' cooperation more effective and ensure that it adequately contributes to ensuing investigations by competent authorities, the current system of "ex post" consent provided on a case-by-case basis, uncertain and lengthy, should be replaced by "a presumption that all the information provided through FIU-to-FIU cooperation should be available to the receiving FIU for domestic dissemination and further use, whenever relevant or appropriate, similar to domestic information".

Similarly, while stating that "the need to obtain authorisation usually delays the processing of the information", a respondent suggests that forms of "ex ante" consent should be adopted, so that the dissemination of the information is confirmed contextually already at the time of the exchange: this FIU informs that it has adopted a formula to grant the prior authorisation within the initial response and suggests that "it would be very beneficial if every FIU in the EU uses the same system of prior authorisation".

On the same point of allowing broader use and dissemination of the information exchanged through FIU-to-FIU cooperation, other respondents go as far as to note that "the current obstacles should be removed and the current prior-consent rule overturned and replaced with a general presumption of possibility to disseminate with potential limited exceptions to be indicated in advance by the providing FIU."

As said, respondents also point out that the consent to use the information exchanged in investigation through appropriate dissemination to relevant agencies is frequently made subject to conditions and refused by requested FIUs when such conditions are not fulfilled. These are cases where the requesting FIU is prevented from making the information received available from relevant investigations, despite its possible relevance for such investigations.

As pointed out by a respondent, "processing information without the possibility to make it available (when relevant) through domestic dissemination frustrates the main purposes served by FIUs and the effectiveness of their analytical functions. This is the case also for information gathered through cooperation with foreign counterparts". Most frequently, based on inputs provided by respondents, the consent is refused when:

- the underlying criminality is not properly identified by the requesting FIU or does not correspond to criminal provisions in force in the country of the requested FIU ("double criminality"[223]);
- the use for which the consent is sought goes beyond the pursuance of "intelligence purposes" (that is aims at using the information in the context of criminal investigations or proceedings).

[223] See also paragraph 6 (as well as, more broadly, Chapter 6, par 2), on the issues surrounding the indication and nature of predicate offences.

In addition, a respondent, recalling Articles 53(3) and 55(2) that allow FIUs not to provide consent for further dissemination where such dissemination would not be in accordance with fundamental principles of national law, has argued that the reference to "fundamental principle of national law" leaves room for different interpretations and implementation and should be further defined"[224].

8.1 Limitations of the use to "intelligence purposes" only

Several respondents recall that the FIUs' capacity to provide the consent to allow further use or dissemination of the information exchanged is generally limited to the pursuance of "intelligence purposes": this entails that the recipient agencies can only employ the information provided by foreign FIUs in support of investigations, without translating this into formal evidentiary material or other elements to be used in the context of formal legal proceedings[225]. As routinely pointed out by FIUs in their exchanges, should the information provided need to be used as evidence in formal prosecutions or proceedings, the FIU-to-FIU exchanges would have to be followed up and "validated" through appropriate mutual legal assistance initiatives among the competent authorities of the countries involved.

Respondents emphasize that this limitation to the use of the information exchanged, and the need to "shift" from the intelligence stage to the law enforcement or judicial stage, pose significant constraints to the effectiveness of FIUs' cooperation, especially in most significant cases where the information exchanged may prove useful to support investigations or to bring prosecutions on money laundering or terrorist financing activities. Moreover, the need to revert to mutual legal assistance channels brings uncertainties and certainly raises issues of timeliness.

On this note, it is observed that this limitation "is highly inefficient as it forces competent authorities to start often laborious MLA procedures to re-obtain the same information already available under a different formal setting".

In addition, an FIU points out, in its feedback to the questionnaire, that the limitation according to which information can be disseminated domestically "only for intelligence purposes", and not for use as evidence in legal proceedings is "not in line with several national systems (especially those of a civil law nature) where prosecutors and judges cannot be constrained as to how they form evidence".

Based on the excessively narrow scope of the FIUs' capacity to provide the consent to use the information exchanged, it is observed that "the usual limitation according to which information can be disseminated domestically 'only for intelligence purposes' and not for use as evidence in legal proceedings should be removed".

[224] See the analysis and consideration on this point in Chapter 6, par. 10.

[225] The issue of information for intelligence purposes only is already being examined by the EU FIU Platform. Following Platform members' interest in scrutinising the meaning of the term "intelligence purposes" (used extensively by a number of regional FIUs in international co-operation), a Project Team was formed to examine it in light of the EU's legislation and Egmont standards. This team's 'Project Report on Use for Intelligence Purposes' was approved at the 10 June 2016 EU Platform meeting. This report concluded that FIUs mostly applied the term 'use for intelligence purposes' to clarify that the provided information can be disseminated to competent authorities, but cannot be used as evidence in future proceedings.

9. Insufficiently motivated requests

Some problems encountered in FIU-to-FIU cooperation are identified in the frequent lack of adequate motivation underlying the requests. As these are often not duly substantiated, the requested FIUs encounters difficulties in providing feedback, both as regards their legal capacity to gather and share information and the practical uncertainties in discerning and identifying relevant the data to provide.

On this point, respondents inform that requests for information frequently lack adequate indications about the links with the countries of the requested FIUs or a description of the underlying cases and of how they relate to money laundering, associated predicate offences or terrorism financing. Responses to the survey also refer to "fishing" requests, that is requests which are addressed to a broad number of counterparts and lack an adequate description and the identification of connections with particular countries; these responses reiterate that FIUs would "highly appreciate a little description of the case that would indicate the reasons of requesting".

Some respondents emphasize that they are in several cases prevented from providing full cooperation due to the insufficient information contained in the requests about the offences (especially money laundering predicate crimes) pursued by the requesting counterparts, particularly as regards their description and their nature. These are cases where, as discussed previously in the Report[226], requested FIUs may be under a requirement, based on domestic laws, to provide cooperation only on sufficiently demonstrated grounds that criminal activity has been identified or, even more narrowly, only in relation to certain categories of offences, notably those specifically covered by domestic legislation (see also previous paragraph 6 in this Chapter).

On this point, it is important to recall that there is certainly a requirement, in international standards and EU provisions, that requests for information should be duly motivated[227]; this requirement includes a need for the requesting FIU to set out the grounds for suspicions of money laundering or terrorist financing at the basis of the ongoing analysis for which cooperation is sought.

At the same time, however, this requirement should not go so far as to expect requesting FIUs to provide information on the identification of particular underlying criminalities and their description. FIUs in fact, as they carry out analysis on suspicions (as opposed to investigations on particular offences), are normally not in a position to identify particular crimes at the early stage where they operate and should therefore not expected to provide such indications. It is also important to recall that cooperation should not be refused on the grounds of the lack of indication about the underlying criminality or of its nature (article 53(1) of the fourth Directive; see also the analysis in Chapter 6 on this point).

10. Cooperation on terrorist financing

Challenges are reported by respondents surrounding FIU-to-FIU cooperation in terrorist financing matters. However, based on responses, while general problems and shortcomings affecting cooperation clearly have an impact also on exchanges related to potential terrorist financing cases, existing difficulties seem related more to the innovative and constantly evolving features of terrorist financing activities than on particular deficiencies in this area in the system of FIUs' cooperation.

[226] See, for example, Chapter 6, par. 2.3.

[227] On this point, for example, article … of the fourth Directive establishes that … More amply, The 'Egmont Principles for Information Exchange between FIUs' (Section C, paragraph 17) state that "when requesting co-operation, FIUs should make their best efforts to provide complete, factual and, as appropriate, legal information including the description of the case being analysed and the potential link with the country receiving the request".

More particularly, respondents seem to flag a need to develop new and more targeted forms of international cooperation specifically capable of detecting financial networks supporting terrorist organisations or individuals seeking to perform or participate in terrorist acts. A need to intensify efforts aimed at detecting suspicions of terrorist financing through international cooperation is also recalled, noting that the vast majority of the exchanges continues to be focussed on money laundering cases. Also, based on domestic legislation and practices, it is felt that greater flexibility should be allowed in sharing information and greater access should be granted to information outside of FIUs.

As relevant background issues, respondents also emphasize that national legislations on terrorist financing may still diverge significantly (for example, in the definition of relevant criminal activities), which potentially affects the operations of FIUs; differences in FIUs themselves, as regards capacities and powers, are also felt as particularly acute: when it comes to carrying out cooperation in the terrorist financing domain, "the differences between the Member State FIUs are a concern; all the EU FIUs are not in the same position".

11. Cooperation on cross border cases

Some respondents have flagged challenges arising from new forms of exchange of information devised by the fourth Directive, notably as regards the requirement to share information on cases that have a cross-border dimension: article 53(1), last paragraph, of the Directive, in fact, makes it an obligation for EU FIUs to forward suspicious transaction reports "that concern another Member State" to the FIU of this Member State[228]. Reactions on this point have been different.

On the one hand, responses recall the need to develop these forms of sharing information by increasing the "spontaneous dissemination of cross border transactions". These are perceived as a useful tool for allowing FIUs to receive information about potential money laundering or terrorist financing activities going on in their countries but reported to counterparts in other countries[229].

A respondent has commented that suspicious activities are being reported to the home FIU "despite [the fact that] they are carried out in another country where the associated money laundering, predicate offences or terrorist financing would materialise and should be analysed, investigated and prosecuted. Currently, FIU-to-FIU cooperation is insufficient to compensate for this loss of information by the authorities in the host country. FIUs of the country where entities operating cross border on a free provision of services basis are located should share this information proactively with interested counterparts". This respondent also adds that "the amount, nature and quality of cross border disclosures received from other EU FIUs still appear insufficient. Major phenomena associated with, for example, money transfer operators acting cross-border and tax offences committed by non-residents are not yet reported"; it is also flagged that it is "important to establish common criteria determining which disclosures concern another Member State".

In this same perspective of the need to foster and develop meaningful cross-border reporting on significant cases of potential criminality, a respondent has voiced concerns over "the amount, nature and quality of cross-border disclosures" from other EU FIUs, considered yet insufficient: in fact, for example, "major phenomena associated with [i.a.] tax offences committed by non-residents are not yet reported".

[228] "When an FIU receives a report pursuant to point (a) of the first subparagraph of Article 33(1) which concerns another Member State, it shall promptly forward it to the FIU of that Member State".
[229] See Chapter 6 for an analysis on the issue of cross-border reports and on how this obligation is currently applied by EU FIUs.

On a different note, other respondents highlight, more on the "providing" than on the "receiving" side, that the obligation to identify and share cross-border reports brings significant difficulties, related to both the current absence of uniform and sufficiently certain criteria and the intrinsic additional workload for FIUs to identify and transmit all relevant disclosures, which is potentially very significant[230].

On this last point, it is observed that, depending on how the requirement to forward cross-border disclosure will be interpreted and implemented (notably, in relation to the scope of "cross-border transactions" which will result), the workload of FIUs is susceptible to change significantly. As the volume of the disclosures that potentially qualify as "concerning another Member State" can be sheer, this may entail a potential substantial shift of activities for FIUs, with more focus cast (and resources dedicated) to these international cooperation tasks.

One respondent goes as far to ask for a "reconsideration or derogation of the last paragraph of Article 53(1)" of the fourth Directive on the requirement to forward cross-border reports, indicating that "no proper impact assessment has been carried out and its implementation threatens to overload the international cooperation unit".

12. Innovative forms of cooperation

Interestingly, one respondent has indicated that "the usual dynamic [of FIUs' cooperation] based on response-to-request is becoming increasingly insufficient vis-à-vis the need to share information a) more amply and b) on an ex-ante perception (that is before, and regardless of, already established links by an FIU which only on this basis can file a request). This traditional approach is proving obsolete and inadequate particularly in facing the new threats of terrorist financing. FIUs should directly inform each other and share information in all cases which can be of interest to counterparts (without waiting for requests)."

13. Lack of timely cooperation

Respondents extensively mention the timeliness of responses as a critical area in FIU-to-FIU cooperation. In several cases cooperation, either the initial exchange of information or the subsequent feedback on the consent requested for further use or dissemination, is not provided in a timely manner, to the detriment of the analytical activities carried out by the requesting FIU and of possible ensuing law enforcement actions.

It is observed on this point that replies to requests "take a long time with certain jurisdictions" (sometimes even more than a year). These delays become particularly significant in "those cases where the requested FIU needs to access or obtain information from external sources" to provide

[230] As recalled in Chapter 6, par.5.1.2, concerns have also been rasied on the feasibility of simply forwarding received STRs/SARs without any further evaluation. The comment received in this respect, has flagged that the STR/SAR received "is only 'information' related to "uncorroborated facts" which "does not become intelligence until it has been assessed and checked against other databases, and then agreed to contain a reasonable suspicion of link to crime or terrorism". The concern is that the FIU "would surely be breaking Human Rights law (right to privacy)" if cross-border STRs/SARs were "sent on to the other MS mentioned without a possible link to crime or terrorism being established. The mere suspicion of the reporter is not sufficent, there has to be an informed/ second opinion view formed".
Difficulties on sharing cross-border STRs/SARs may also derive from existing differences among national definitions, nature and content of suspicious-based disclosures. As recalled in Chapter 3, par. 2.6, due to these differences, FIUs exchange cross-border reports that are different under several respects and may not even be "recognized" or usable by the recipient counterparts (for example, in cases where the disclosure forwarded focuses on predicate offences whereas the receiving FIU can only act upon information on proceeds and on the related money laundering).

the requested cooperation. It is also indicated that the fact that the required information is not provided in a timely manner means that the case concerned may have to be closed "or, in cases of urgent requests, transactions must be released".

The problems associated with delays in receiving feedback on the request for consent to further using or disseminating the information exchanged, also flagged by respondents particularly as regards their impacts on pending law enforcement actions, have been highlighted in paragraph 8. It is also important to recall the different evidence gathered through the section of the Survey dedicated to capacity of EU FIUs' to provide timely cooperation: responses suggest that feedback is normally given in a timely manner. See, on this point, the discussion in Chapter 6, par. 1.9, on the different viewpoints taken by FIUs in responding to different sections of the Survey (as providers or as requestor of cooperation) and the need to set up a common system for collecting data and statistics which are uniform and comparable across Member States and allow to measure on objective bases the performance of EU FIUs in exchanging information in a timely manner.

A respondent makes an interesting consideration on how delays in providing cooperation may depend, at least in part, to the FIUs' internal prioritization of tasks which privileges domestic cases and analyses which, in turn, derives from the disconnection between the cooperation provided to foreign counterparts and the FIU's own analytical activities (and associated priorities): the insufficient timeliness of responses appeared "to be connected with the circumstance that too often in FIUs' internal organisation the function of entertaining international exchanges, especially by responding to foreign requests, is not conducted together with an appropriate analytical activity and, as a consequence, is given a lower priority (less resources, longer timeframes)".

The issue of whether FIUs assign low(er) priority to cooperation in favor of foreign counterparts, with respect to own domestic analysis, could be emphasized. Especially in a context where the volume of activities and the tasks assigned to FIUs increase, with an associated increase in the timeframe for providing cooperation, further analysis may be dedicated to this issue, with particular focus on understanding whether the right incentives are in place for FIUs to provide timely cooperation.

The difficulties that EU FIUs encounter in providing cooperation in a timely manner may be associated with the challenges that are posed by the increase in the FIUs' workloads which, as flagged by respondents, is particularly significant in the international cooperation area (see the following paragraph).

14. Problems in cooperation in situations of postponement of transactions

Respondents flag two different issues related to cooperation between FIUs in situation of postponement of transactions: a) difficulties in obtaining the postponement of transactions by foreign FIUs in cases of cross-border flows of funds; b) difficulties in ensuring fast enough cooperation when a transaction has been postponed and urgent decisions have to be taken on the follow-up.

Under the first perspective, difficulties are reported in obtaining meaningful cooperation from foreign FIUs in cases where the requested cooperation aims at blocking transactions abroad: particularly in case of transfer of illicit funds to other countries, if the FIUs of such countries "are not in a position to freeze such monies, then such monies [are] at risk of being absconded before an official request for mutual legal assistance [can be] processed".

Under the second perspective highlighted above, some respondents refer to difficulties in ensuring adequate cooperation in situations where the requesting FIU has adopted a postponement order blocking the transactions for which cooperation is requested. In these cases, in fact, feedback has to be provided in a very short timeframe, within which the transactions and the underlying assets have to be either seized (based on order by the competent authorities) or released, and this poses significant challenges to effective cooperation.

In this regard, some respondents highlight that major difficulties derive from the fact that FIUs have "the authority to issue orders for freezing of funds for an extremely limited period of time. One, three, or even five days are not enough to perform the necessary analysis, exchange intelligence with a foreign FIU and a national LEA, and prepare a mutual legal assistance request".

15. Increase in FIUs' workload

Respondents also emphasize that the implementation of the new provisions and obligations in the fourth Directive is likely to bring about additional tasks and increased workloads for FIUs, on several fronts.

A respondent recalls how the activities related to FIU-to-FIU cooperation are increasing in volumes and intensity: in the last couple of years it has been noted "a steady increase in the numbers of requests sent and received. The number of sent requests has doubled since 2012, the number of received inquiries tripled. Adding the large increase of reports providing a spontaneous dissemination of information from foreign FIUs, the Unit's staff is reaching its full capacity in reference to handling international exchange of information".

Another respondent also specifically voice concerns related to expected pressure on resources deriving from international cooperation duties, in general, and cross-border transactions sharing, specifically (see paragraph 11): an "increase in the workload regarding the exchange of information" has been noted; moreover, "Articles in the 4AMLD increase the workload in this aspect. Hence there is going to be the need to allocate more resources to this task in a short term, given that there is an obligation to process the request without undue delay".

More specifically, an FIU has noted that "there is a significant workload coming from some FIUs that use their foreign counterparties as a way to obtain information on accounts or assets of people that have already been subject to a criminal proceeding. So the role they are playing is out of the core functions an FIU should have".

16. Difficulties deriving from the absence of reciprocity

Some respondents mentioned difficulties encountered in FIU-to-FIU cooperation due the lack of the reciprocity conditions. The responses to the survey on this point assume "reciprocity" as the capacity of counterparts to exchange the same information, and exercise the same powers to access it, as the requesting FIU.

It is noted, in fact, that "there is lack of reciprocity (…) as regards the information that can be shared"; for example, "some FIUs still do not have access to bank accounts holders nor can obtain banking and financial information", and this is felt as "a very relevant shortcoming". Other responses refer to difficulties in "receiving adequate cooperation (especially on financial information) from FIUs that act as police bodies and conduct investigations".

Importantly, as more amply discussed in Chapter 6, the lack of reciprocity can trigger refusals to exchange information with counterparts that an FIU has reason to believe would not be in a position to provide the same cooperation if requested on a similar case or under similar circumstances.

17. Use of FIU.NET

Some respondents flag the need to expand and intensify the use of FIU.NET, both as regards the range of participating FIUs and the functionalities available in support of the FIU-to-FIU cooperation. These responses, in particular, mention that "would be useful to encourage EEA FIUs to join the FIU.NET", complain that the "Ma3tch" system is not yet fully implemented, invite to develop "the use of FIU.NET and its functionality".