Council of the
European Union

Brussels, 22 July 2021
(OR. en)

10290/21
ADD 2

Interinstitutional Files:
2021/0239 (COD)
2021/0240 (COD)
2021/0241 (COD)
2021/0250 (COD)

EF 227
ECOFIN 664
DROIPEN 122
ENFOPOL 259
CT 95
FISC 110
COTER 85
CODEC 1004

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	22 July 2021
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2021) 190 final
Subject:	COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Anti-money laundering package: - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU)2015/849 - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Authority for Countering Money Laundering and Financing of Terrorism, amending Regulations (EU) No 1093/2010, (EU) 1094/2010 and (EU) 1095/2010 - Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets

Delegations will find attached document SWD(2021) 190 final.

Encl.: SWD(2021) 190 final

EUROPEAN
COMMISSION

Brussels, 20.7.2021
SWD(2021) 190 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the

Anti-money laundering package:

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive (EU)2015/849

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Authority for Countering Money Laundering and Financing of Terrorism, amending Regulations (EU) No 1093/2010, (EU) 1094/2010 and (EU) 1095/2010

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets

{COM(2021) 420 final} - {SEC(2021) 391 final} - {SWD(2021) 191 final}

Table of Contents

1 INTRODUCTION: POLITICAL AND LEGAL CONTEXT 1

2 PROBLEM DEFINITION 7

2.1 What is/are the problems? 7

2.2 What are the problem drivers? 13

2.2.1 Lack of clear and consistent rules 14

2.2.2 Inconsistent supervision across the internal market 18

2.2.3 Insufficient coordination and exchange of information among FIUs 19

2.3 How will the problem evolve? 20

3 WHY SHOULD THE EU ACT? 23

3.1 Legal basis 23

3.2 Subsidiarity: Necessity of EU action 24

3.3 Subsidiarity: Added value of EU action 24

4 OBJECTIVES: WHAT IS TO BE ACHIEVED? 25

4.1 General objectives 25

4.2 Specific objectives 25

5 WHAT ARE THE AVAILABLE POLICY OPTIONS? 26

5.1 What is the baseline from which options are assessed? 26

5.2 Description of the policy options 27

5.2.1 Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards 27

5.2.2 Improve the effectiveness and consistency of anti-money laundering supervision30

5.2.3 Increase the level of cooperation and exchange of information among Financial Intelligence Units 32

6 WHAT ARE THE IMPACTS OF THE POLICY OPTIONS AND HOW DO THEY COMPARE?. 33

6.1 Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards 33

6.2 Improve the effectiveness and consistency of anti-money laundering supervision 40

6.3 Increase the level of cooperation and exchange of information among Financial Intelligence Units 43

7 PREFERRED OPTIONS 45

7.1 Effectiveness 45

7.2 Efficiency 46

7.3 Coherence 47

7.3.1 General remarks on coherence *47*

7.3.2 Coherence between the preferred options and other Commission policies *47*

The draft regulation on crypto-assets provides a legal framework for crypto-assets and crypto assets services providers, including a definition of 'crypto-assets' and a list of recognised crypto-asset services that transposes in the EU law the recommendations of the Financial Action Task Force. Other provisions of the draft regulation on licensing and registration requirements, rules for supervision, preservation of financial stability and investors protection will be cross-referred in this legislative proposal. *49*

7.3.3 Coherence between the preferred options and the EU data protection framework49

7.4 Summary of impacts of selected options 52

8 REFIT (SIMPLIFICATION AND IMPROVED EFFICIENCY) 52

9 HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED? 53

ANNEX 1: PROCEDURAL INFORMATION 56

ANNEX 2: STAKEHOLDER CONSULTATION 58

ANNEX 3: WHO IS AFFECTED AND HOW? 66

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE 66

2. SUMMARY OF COSTS AND BENEFITS 68

INCREASED EFFECTIVENESS OF AML/CFT RULES, CONSISTENT SUPERVISION ACROSS THE INTERNAL MARKET AND EFFICIENT EXCHANGE OF INFORMATION AMONG FIUS IS THE MAIN OBJECTIVE OF THE INITIATIVE. THIS SHOULD REDUCE THE QUANTITY OF ILLICIT FUNDS WHICH ARE LAUNDERED OR USED TO FINANCE TERRORISM, EITHER THROUGH GREATER DETECTION OR DETERRENCE. 68

PREFERRED OPTIONS: 68

- *ENSURE A GREATER LEVEL OF HARMONISATION IN THE RULES THAT APPLY TO ENTITIES SUBJECT TO AML/ CFT OBLIGATIONS AND THE POWERS AND OBLIGATIONS OF SUPERVISORS AND FIUS.* 68

- *DIRECT SUPERVISORY POWERS OVER SELECTED RISKY ENTITIES IN THE FINANCIAL SECTOR SUBJECT TO AML/ CFT REQUIREMENTS AND INDIRECT OVERSIGHT OVER ALL OTHER ENTITIES.* 68

- *THE EU FIUS' PLATFORM TO BECOME A MECHANISM AS PART OF THE AML AUTHORITY, WITH POWER TO ISSUE GUIDANCE AND TECHNICAL STANDARDS AND TO ORGANISE JOINT ANALYSES AND TRAINING, CARRY OUT TRENDS AND RISK ANALYSIS.* 68

ANNEX 4: EVALUATION 71

ANNEX 5: EU AML AUTHORITY: ORGANISATIONAL INSTITUTIONAL, RESOURCE AND BUDGET ISSUES 75

ANNEX 6: AREAS FOR GREATER HARMONISATION OF RULES 80

ANNEX 7: INTERCONNECTION OF BANK ACCOUNT REGISTERS 90

ANNEX 8: EU POLICY TOWARDS THIRD COUNTRIES WITH STRATEGIC DEFICIENCIES IN THEIR AML/CFT REGIMES 103

ANNEX 9: INTRODUCTION OF CASH LIMITS 108

Glossary

Term or acronym	*Meaning or definition*
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Agency/Authority (not yet in existence)
AMLD	Anti-Money Laundering Directive (Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended by Directive (EU) 2018/843)
BO	Beneficial Owner (natural person who ultimately benefits from a registered company, often indirectly via a chain of companies)
CASP	Crypto Asset Service Provider
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
EBA	European Banking Authority
EDD	Enhanced Due Diligence
ESMA	European Securities and Markets Authority
Europol	European Union Agency for Law Enforcement Cooperation
FATF	Financial Action Task Force (international standard-setting body in the field of AML/CFT)
FIU	Financial Intelligence Unit (national enforcement body which receives STRs from OEs and forwards them, as appropriate to criminal investigation authorities)
GDPR	General Data Protection Regulation
HRTC	High Risk Third Country
KYC	Know Your Customer
ML	Money Laundering
OE	Obliged Entity (legal or natural person within the scope of AMLD and subject to AML/CFT rules)
SNRA	Supranational Risk Assessment
SRB	Self-Regulatory Body (e.g. bar association)
SSM	Single Supervisory Mechanism
STR	Suspicious Transaction Report
TF	Terrorism Financing

1 INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Money laundering is the process through which proceeds of crime, their true origin and ownership, are changed so that they appear legitimate. Together with terrorism financing it represents an ongoing challenge to the integrity of the European Union (EU) financial system and the security of its citizens.

Combating money laundering and terrorist financing has been part of the European Union political agenda for over thirty years. In this time the EU has developed a regulatory framework, going beyond the international standards adopted by the Financial Action Task Force[1] (FATF), to prevent and manage the associated risks. This framework must continuously evolve to keep pace with growing sophistication of financial crime, technological developments allowing for new means to launder money and the increasing openness of the EU Internal Market.

The first EU anti-money laundering Directive[2] (AMLD) was adopted in 1991. It applied only to financial institutions and focused on combatting the laundering of proceeds from drug trafficking. The AMLD has since undergone three major reforms (in 2001, 2005 and 2015) and substantial amendments in 2018. Today, it addresses the prevention of money laundering as a result of all serious criminal offences and lays down obligations for a number of non-financial activities and professions including lawyers, notaries, accountants, estate agents, art dealers, jewellers, auctioneers and casinos. The concept of beneficial ownership has been introduced to increase transparency of complex corporate structures, and enforcement follows a risk-based approach to focus resources where risks are the highest.

Since 2017, during the implementation phase of AMLD4 and AMLD5, a number of high-profile alleged money laundering cases have surfaced across the EU, involving billions of euro laundered through EU credit institutions or with the involvement of professionals and undertakings operating outside the financial sector, such as auditors, tax advisors and trust and company service providers. These prominent alleged cases[3] revealed structural weaknesses of the current system. The limitations of the current framework were analysed and summarised in the July 2019 package of Commission documents[4] concerning anti-money laundering and countering the financing of terrorism,

[1] The Financial Action Task Force (FATF) is the global money laundering and terrorist financing standard-setter, created in 1986, with the European Commission and 14 Member States as members.

[2] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering

[3] For example, the Danske Bank case involved an estimate of EUR 200 billion in suspicious transactions, while the Swedbank case concerned around EUR 37 billion worth of suspicious transactions.

[4] Communication from the Commission - Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework (COM/2019/360 final), "post-mortem report" referred to in the next footnote, Supranational Risk Assessment (COM/2019/370 final), and report on FIU cooperation (COM/2019/371).

including a so-called '*post-mortem*' report on alleged money laundering cases involving EU banks[5]. The obtained evidence points to a fragmented, inconsistent and uncoordinated implementation and application of EU anti-money laundering rules. The 2019 Communication concluded that the problems identified were of a structural nature and could not be remedied by the most recent review of EU rules in this area (the 5th Anti-Money Laundering Directive of 2018).

This view is supported by the European Parliament and the Council. In its resolution of 19 September 2019, the European Parliament called for more impetus to be given to initiatives that could reinforce AML/CFT actions at EU level and for speedy transposition of EU rules by Member States[6]. On 5 December 2019, the Economic and Financial Affairs Council (ECOFIN) adopted conclusions on strategic priorities for AML/CFT[7], inviting the Commission to explore actions that could enhance the existing framework.

In light of the priority that AML/CFT represent for the EU under the priority of the von der Leyen Commission "An economy that works for people", the Commission presented on 7 May 2020 an Action Plan[8] for a comprehensive Union policy on preventing money laundering and terrorism financing. The Action Plan sets out the measures that the Commission will undertake to better enforce, supervise and coordinate the EU's rules on combating money laundering and terrorist financing, with six priorities or pillars:

1. Ensuring the effective implementation of the existing EU AML/ CFT framework,
2. Establishing an EU single rulebook on AML /CFT,
3. Bringing about EU-level AML/ CFT supervision,
4. Establishing a support and cooperation mechanism for FIUs,
5. Enforcing EU-level criminal law provisions and information exchange,
6. Strengthening the international dimension of the EU AML/CFT framework.

The first pillar is being implemented by the Commission's ongoing transposition and compliance control of the existing AML/CFT rules. Since January 2020, when the most recent EU AML/CFT rules had to be transposed, the Commission has opened 23 infringement cases for non-communication or partial communication of transposition. In parallel, the Commission referred three Member States to the European Court of Justice and issued five reasoned opinions for incomplete transposition of the AML/CFT rules adopted in 2015. Four Member States received letters of formal notice for failing to

[5] Report from the Commission on the assessment of recent alleged money laundering cases involving EU credit institutions, COM/2019/373 final.
[6] Reference 2019/2820/RSP. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_EN.html.
[7] Reference 14823/19. Available at: https://data.consilium.europa.eu/doc/document/ST-14823-2019-INIT/en/pdf.
[8] Communication from the Commission - Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (C(2020) 2800 final)

correctly transpose such measures. Moreover, the Commission proposed in May 2020 that the Council issue recommendations on AML/CFT for eleven Member States under the European Semester exercise. The Commission has also requested the Council of Europe to carry out an assessment of the implementation of the current rules in Member States. Administrative letters have already been addressed to those Member States for which the assessment by the Council of Europe has been completed to follow up on any issues detected.Beyond these areas, enforcement action continues, with the actions covered by the Council's 2018 AML Action Plan being almost fully completed, leading to better understanding and coordination among prudential and AML authorities in the financial sector. One of the key focus areas will be the reduction of divergences among Member States and the establishment of common rules that apply throughout the Union. In future, directly applicable rules in a Regulation will remove the need for transposition and reduce delays in the application of EU rules, whilst also freeing up resources for enforcement purposes.

However, better implementation of the current rules alone is not sufficient. In view of the nature of the identified problems, the current AML/CFT framework requires a reform that aims to ensure a more uniform implementation of the rules across the EU, by reducing the margin of interpretation left to Member States and by making the implementation and application of the rules more consistent across the internal market. This requires a structural change as well as introduction of new rules. To this end, the Action Plan contains a commitment to propose legislation in Q1 2021 to create a single rulebook, set up an EU-level AML/CFT supervisor, and to establish an EU coordination and support mechanism for FIUs, in all cases "based on thorough impact assessment of options"[9]. This present impact assessment therefore focusses on pillars 2, 3, 4 and in part pillar 6 of the Action Plan.

In relation to the fifth pillar, the Commission will issue guidance and share good practices for the public-private partnerships between entities subject to AML/CFT obligations and public authorities. The sixth pillar, which is discussed in annex 8, concerns inter alia a more granular risk based approach by requiring obliged entities to apply enhanced customer due diligence to certain transactions with certain third countries. It also provides for a stronger role of the European Union in the Financial Action Task Force (FATF). As the global standard-setter in the AML/CFT field, the FATF develops recommendations to ensure resilience of the financial system against criminals trying to misuse it for money laundering, terrorist financing or proliferation financing purposes. These standards largely serve as inspiration for national AML/CFT legislation. More and more, EU standards are going beyond FATF standards, and in

[9] This urgency reflects "growing consensus that the framework needs to be significantly improved. Major divergences in the way it is applied and serious weaknesses in the enforcement of the rules need to be addressed" (Action Plan, Introduction). This consensus is reflected in the responses to the public consultation on the Action Plan summarised at annex 2.

recognition of this the Action Plan advocates for a stronger role of the EU in the FATF to shape international standards.

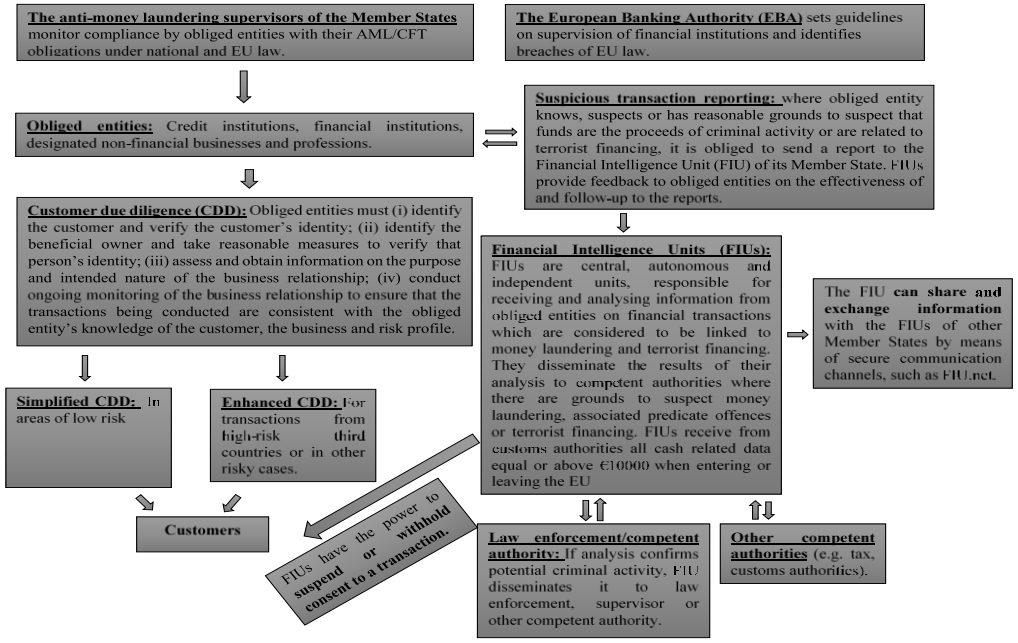
The positioning of the co-legislators in favour of a bold reform of the EU AML/CFT framework, echoed by the vast majority of stakeholder that responded to the Commission's public consultation, indicate that there is a clear understanding and willingness from all sides that the EU should do more in this area. On 4 November 2020, the ECOFIN Council adopted further Conclusions supporting each of the pillars of the Commission's Action Plan[10]. Such further action should address structural weaknesses of the EU AML/CFT framework and enhance its capacity to effectively counter money laundering and terrorist financing so as to reduce the exposure of our financial system to such risks and improving the functioning of the internal market.

While the current reform does not touch aspects pertaining to investigations and prosecutions of criminal cases, nor freezing/confiscation of criminal assets, the planned changes to the preventative framework will contribute to the quality and relevance of information provided to law enforcement authorities and increase the rate of transaction freezing in view of the opening of a case. It is however important to note that other factors outside the scope of this reform affect investigation and prosecution, including the prioritisation of money laundering cases by law enforcement and prosecutors and the effectiveness of national judicial systems (e.g. overload of cases).

The general principle of free movement of capital enshrined in Article 63 TFEU does not exclude that Member States and/or the European Union have a monitoring role on capital movements. Protection of citizens against activities for money laundering purposes is necessary and it has been long seen as one of the exceptions to the free movement of capital by the Court of Justice of the EU (the "Court")[11].

[10] 12608/20. Available at https://data.consilium.europa.eu/doc/document/ST-12608-2020-INIT/en/pdf
[11] C-358/93 - Bordessa and others, § 21-22.

Box 1: How does the EU Anti-money laundering framework work?



Box 2: The architecture of the EU AML/CFT framework

This architecture comprises several private and public sector actors, tasked with specific but interrelated roles. The framework has a preventive and a repressing arm.

The AML/CFT preventive policy aims at the prevention of ML/TF by the setting of specific obligations for financial institutions and certain non-financial institutions and professionals. By virtue of their activity, these entities are well placed to intercept those transactions and operations that criminals need to carry out in order to conceal and integrate illegal money into the legitimate economic and financial environment. Therefore, such entities are subject to specific obligations. On the one hand, they are required to carry out customer due diligence to identify and verify the identity of customers and beneficial owners, to obtain information on the business relationship and to monitor it. On the other hand, they are obliged to report transactions in case they identify any suspicion. The scope and nature of these obligations is based on the intrinsic risk posed by clients, transactions and nature of the business relationship (risk-based approach).

National AML supervisors are tasked with ensuring compliance with these requirements. The intensity of supervision is based on the degree of risk that a given entity incurs. Supervisors have to make sure that entities' internal controls and compliance procedures are commensurate to AML/CFT risk. National supervisors must cooperate with their counterparties in other jurisdictions for the supervision of cross-border entities.

In the financial sector, AML supervision in Member States is often concentrated in a single public authority. While AML supervision is always a distinct function from prudential supervision, a number of Member States have a single authority carrying out both types of supervision of some or all financial sector entities. In many Member States the Financial Intelligence Units have supervisory powers over at least some financial sectors. In a few Member States certain non-financial sectors are supervised by a self-regulatory body, such as the bar association.

Suspicious transactions are reported to Financial Intelligence Units (FIUs). FIUs are central national units, responsible for receiving and analysing information from private entities on transactions which are suspected to be linked to money laundering and terrorist financing, as well as for receiving cash-related data from customs authorities. FIUs exchange information amongst themselves by means of secure communication channels, such as FIU.net. They disseminate the results of their analyses to law enforcement and tax authorities for further investigations and prosecution where there are grounds to suspect money laundering, associated predicate offences or terrorist financing, and can order temporary freezing of transactions. FIUs provide feedback to private entities on effectiveness of and follow-up to reports of suspected ML/TF.

The AML/CFT repressive policy aims at punishing criminals through the application of criminal law and the imposition of measures such as seizure, definitive freezing of transactions and confiscation of assets[12]. FIUs, Law Enforcement Agencies (LEAs) and judicial authorities play a

[12] In addition, Directive (EU) 2018/1673 on combating money laundering by criminal law establishes minimum rules concerning the definition of criminal offences and sanctions in the area of money laundering.

prominent role. LEAs receive relevant information and analysis from FIUs and, if there are sufficient grounds, they can open a criminal investigation.

Box 3: Other EU laws that interact with the AML Directive (see also section 7.3)

- The Payment Services Directive (2015/2366) and Electronic Money Directive (2009/110), with the aim to determine the status of agents and distributors and Account Information Service Providers as obliged entities.
- The Payment Accounts Directive (2014/92), with the aim to clarify that suspicion of AML, as a justification to derogate from the obligation to provide a basic account, should be based on case by case/personalised CDD so as not to undermine the right of customers, in particular the vulnerable ones (to a basic account).
- The Deposit Guarantee Schemes Directive (2014/49), with the aim to reduce the risk that suspicious depositors are reimbursed in the pay-outs by deposit guarantee schemes and reconcile the objective of the fight against money laundering and terrorist financing with the protection of depositors and of financial stability.
- EU regulations on restrictive measures ("targeted financial sanctions") covering the EU financial sanctions policy (terrorism, proliferation financing or other types of financial sanctions).
- The Cash Controls Regulation (2018/1672) laying down a system of controls where cash of 10 000 EUR or more need to be declared to Customs when entering or leaving the EU
- Wire Transfer Regulation (2015/847): the application of this Regulation to transfers of virtual assets will be amended by the current package as described in Annex 6, part 8 (introduction of the FATF "travel rule").

2 PROBLEM DEFINITION

2.1 What is/are the problems?

Money laundering and the financing of terrorism pose a serious threat to the integrity of the EU economy and financial system and the security of its citizens. In September 2017, Europol warned that between 0.71 and 1.28% of the EU's annual Gross Domestic Product is '*detected as being involved in suspect financial activity*'[13]. In 2019 alone, this amounted to a value of between EUR 117 and 210 billion of suspicious activities and transactions occurring through the EU's financial system and economy. Only a minor share of these suspicious transactions and activities are detected, with about 2% of assets seized and only 1% ultimately confiscated, allowing criminals to invest into expanding their criminal activities and, ultimately, infiltrate the legal economy.[14] While this low rate of effectiveness is linked to a number of other factors such as prioritisation of

[13] Europol Financial Intelligence Group, *From suspicion to action* (2017)
[14] Europol, Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014, 2016, available at: https://www.europol.europa.eu/publications-documents/does-crimestill-pay.

investigations and duration of court proceedings, some shortcomings pertain to the preventive aspect of anti-money laundering, as discussed in the Commission's 2019 Communication and 2020 Action Plan.

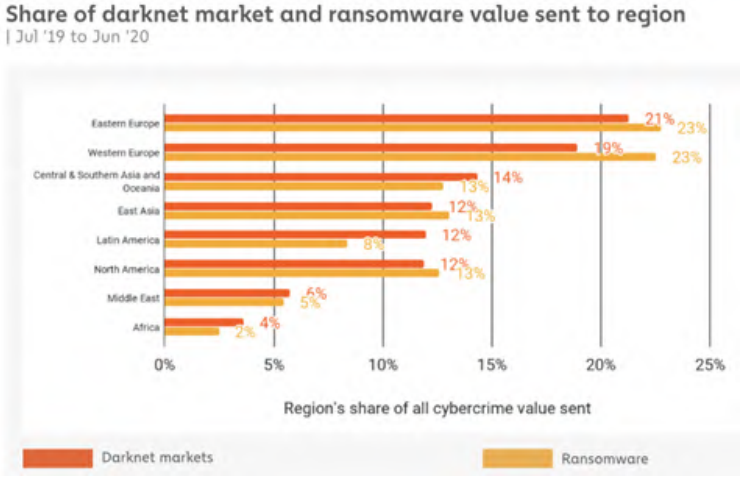
First, **the application of AML/CFT rules across the EU is both ineffective and insufficient**. The 2019 Commission '*post-mortem*' report on the assessment of recent alleged money laundering cases involving EU credit institutions[15] points to a number of deficiencies in the application of AML/CFT measures by the private sector. While these were sometimes the result of neglect or excessive risk appetite by private operators, the report also notes how they link directly to the lack of clarity in current EU rules, which leads to divergent application.

Useful insights into such divergences are provided by credit institutions operating in several EU countries. For example, following media revelations regarding its involvement in alleged money laundering cases, Swedbank commissioned a report from the law firm Clifford Chance to investigate its internal anti-money laundering measures, which it released in March 2020[16]. The report notes for example how the different branches and business lines of Swedbank diverged in their assessment of the risks related to specific transactions, clients and products, resulting in different levels of scrutiny into (prospective) clients and the nature of the business relationship. This in turn led to inconsistent decisions regarding whether to open and maintain a business relationship and the identification and reporting of suspicious transactions and activities. As a result of these shortcomings, the report identifies payments worth EUR 37.7 billion carrying a high risk for money laundering that were made through Swedbank's Baltic subsidiaries during 2014-2019.

The scope of the current rules is also ineffective in dealing with new threats arising from innovation. As Europol notes,[17] the growing popularity and adoption of cryptocurrencies has also led to their increasing use in money laundering schemes. While the EU had paved the way internationally in imposing AML/CFT obligations on providers involved in the transfer between fiat currency and crypto assets, criminal schemes have evolved and are resorting to more complex solutions to launder money, going beyond the services currently covered by EU AML/CFT rules. The EU's exposure to risks related to cryptocurrencies is confirmed in the Chainalysis 2020 Geography of Cryptocurrency Report, which notes that both Eastern and Northern/Western Europe have similar and substantial illicit cryptocurrency activity, and estimates that about 1 percent of Northern and Western Europe's cryptocurrency activity is illicit. The report indicates that "both regions receive similar, high shares of all funds sent from addresses associated with

[15] See footnote 5 above.
[16] https://internetbank.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE57526786
[17] IOCTA – Internet Organised Crime Threat Assessment 2019.

darknet[18] markets and ransomware[19] attacks, [and they] are largely receiving these funds from the same specific criminal entities."



Chainanalysis, 2020 Geography of Cryptocurrency Report

Finally, the current rules are ineffective in ensuring adequate protection of the EU's financial framework while allowing legitimate transactions to take place. For example, the European Banking Authority (EBA) found[20] that under the current framework, in the absence of a conviction or formal charge, there is no public authority that can act to stop a pay-out to a client even if there are indications that the failing credit institution was set up to facilitate money laundering. On the other hand, in another opinion EBA also found that a narrow focus on compliance with customer identification and verification requirements appears to have contributed to certain customers, in particular vulnerable ones, being excluded from access to and use of payment accounts with basic features[21].

This is also true in relation to supervisory activities. In the absence of an explicit link between ongoing supervision and ML/TF risk, not all supervisors consistently take ML/TF concerns into account, and when they do, not all act on these risks in a timely and effective manner. Such failure has been a major contributing factor to serious AML/CFT failures in recent years. Furthermore, there is uncertainty regarding the extent to which a

[18] The darknet (or dark web) is a term used to collectively identify those internet sites only accessible by a specialized web browser, used to keep internet activity anonymous. Such anonymity, while not exclusively sought by criminals, allows illegal activities to be performed without trace.
[19] Malicious softwares designed to block access to a computer system (malware) until a sum of money is paid (hence the term "ransomware").
[20] EBA report on the future AML/CFT framework in the EU (EBA/REP/2020/25)
[21] Opinion of the European Banking Authority on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories (EBA-Op-2016-07)

prior sanction for AML/CFT breaches or a final decision of the supervisor identifying the AML/CFT breaches would be a precondition for a withdrawal of authorisation of a financial institution.

Second, **insufficient oversight of how entities subject to AML/CFT rules apply them** also affects the protection of the EU's internal market and financial system from criminals. While legal obstacles to cooperation among national supervisors have been removed, the level of coordination is left to the individual authorities to decide, and has been limited so far due to a focus on national risks. As shown in the Commission's *post-mortem* report, this has allowed criminals to turn these shortcomings to their advantage.

Example: Danske Bank

One example of the limits of such arrangements is the alleged money laundering case involving Danske Bank's Estonian branch, where suspected payments worth EUR 200 billion were processed for non-resident clients between 2007 and 2015. The lack of cooperation between the Danish and Estonian supervisors in this case was revealed in a series of public statements by the two authorities.[22] This affected their capacity to intervene to remedy the shortcomings in the bank. In fact, despite the regulatory measures taken since 2015, the remedies imposed did not prove sufficient and the Estonian AML/CFT supervisor had to order the bank to close its Estonian operations in 2019. While more recent cases have seen better cooperation between national AML/CFT supervisors, such a voluntary approach is insufficient to ensure that all entities implement in a coherent and effective manner common rules and are all subject to supervision of the highest quality.

The insufficient intensity of supervision is even more apparent in the case of entities subject to AML-CFT rules in the non-financial sectors. Data submitted for 2019 indicate that in a third of Member States no or close to no inspection was performed on accountants and tax advisors, lawyers or trust and company service providers. In some Member States, all these inspections were followed up by an instruction or remedial measure, while in other Member States no action was taken upon any inspection. The sanctions imposed vary significantly for the same group of professionals and breaches from one Member State to another (EUR 2 000 - 30 000). Overall, the intensity of supervisory measures remains insufficient to oversee adequate application of AML/CFT rules by these professionals, which continues to be lower than in the financial sector. Country A provides an example in this sense. In 2019, it performed twice as many inspections on financial institutions than on non-financial entities. Yet, twice as many breaches of AML/CFT rules were detected in the inspections covering the non-financial sector.

Furthermore, risk-based supervision is seldom applied when supervision is delegated to self-regulatory bodies (SRBs) with no or close to no public oversight over their work, as the examples below from Member States show.

[22] https://www.dfsa.dk/News/Press-releases/2019/Report-on-the-Danish-FSAs-supervision-of-Danske-Bank-as-regards-the-Estonia-case
https://www.fi.ee/en/news/response-report-danish-fsas-supervision-danske-bank

Examples from Member States (anonymised) – supervision by self-regulatory bodies

Country B regulates the provision of trust and company services, which require registration and authorisation. Legal professionals are also authorised to operate as trust and company service providers under the supervision of the SRB. This service is considered more exposed to ML/TF risk but the SRB does not collect statistics to identify who are the professionals requiring more intense supervision.

In **country C**, the SRB does not keep data on the number of inspections where AML/CFT breaches were detected, nor of the instructions/warning issued following inspections. The SRB does not keep data on the aggregated number of high-risk costumers a professional would have either, as it considers this against the secrecy obligation.

In response to the public consultation, one national supervisor concluded that "*the FATF MER process has demonstrated that the AML/CFT supervision of [the non-financial sector] is often of a lower standard than that of financial institutions. FATF has specifically stated that the supervision of CASPs should not be carried out by [SRBs] – this appears to be explicit recognition that the AML/CFT supervision by SRBs has not been of the expected or required standard*".

This results in a situation where the number of suspicious transactions or activities reported by these professionals, with the exception of gambling operators and notaries in some Member States is extremely low (e.g. for some professions, such as trust and company service providers, the number of suspicions reported is rarely above 20 and often in the single digit), and they might act as enablers that criminals exploit to launder money. For example, the Slovak FIU indicated that no notary or other professionals involved in the provision of company services reported any suspicions regarding the acquisition of companies or real estate in the country by the convicted Italian mafia member whom journalist Ján Kuciak was investigating prior to his murder. As such, the criminal's investments in about fifty companies were allowed to go unnoticed, and only banks, not other entities such as accountants or real estate agents, reported suspicious transactions that involved him.[23]

Third, **insufficient detection of suspicious transactions and activities by Financial Intelligence Units (FIUs)**, particularly in cross-border cases, limits their capacity to suspend transactions and to disseminate relevant information to competent authorities and other FIUs quickly and effectively so that money laundering and where possible also the related predicate offences can be stopped. Despite the significant amount of suspicious reported to EU FIUs in 2019 (on average about 50 000 per FIU, but with significant divergences between them), less than half of them were actively followed up, and about 70 transactions were suspended on average (for an average total value of 60

[23] Information shared by the Slovak FIU and prosecutors during the country visit for the 2020 European Semester cycle. The number of companies in which the 'Ndrangheta member invested is confirmed by the investigative platform Investigace (https://www.investigace.eu/italian-farms-slovak-soil/).

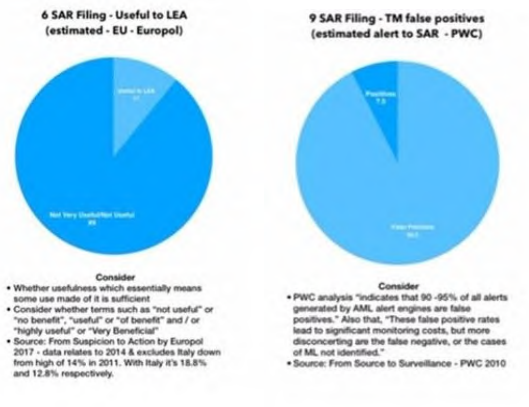
million EUR). Extrapolating these averages to all FIUs, these figures indicate that, at best, the ratio between suspicious flows stopped at an early stage and estimated proceeds laundered within the EU is 1:100.

The number of suspicious transactions and activities reported by the private sector continues to grow since 2014.[24] At the same time, the capacity in FIUs to cope with these volumes of data has not increased commensurately, and only a couple of FIUs reported to the Commission having witnessed substantial increases in their budget and staffing. Despite this, data submitted indicate that FIUs tend to analyse all suspicious transactions reported to them. This has an impact on a significantly increasing backlog, on the speed of their analysis and on their capacity to identify from this amount of data transactions of significance, which also affects the exchange of information between them.

The inadequate feedback from FIUs to private sector entities acting as obliged entities, in particular given the cross-border nature of many transactions, perpetuates this negative cycle. Indeed, only in a minority of cases did the FIUs report providing elaborate feedback on trends and typologies in money laundering tailored to specific categories of obliged entities. Left without information on trends in money laundering and terrorism financing, private sector entities are unable to detect those activities and transactions that are genuinely suspicious and to improve the quality of the information reported. As such, reporting has become an automated process, leading to an increase in reports of no significance (the so-called 'false positives'). Indications confidentially provided by credit institutions to the Commission estimate that between 50% and 75% of reports submitted to FIUs would fall under this category. The sector also shared that based on existing studies the level of false positives could be even higher, as shown in the graphs below which point to around 10% of all STRs submitted as being of use.

[24] For example, suspicious transactions reported to the Finnish FIU increased by 64.2% in 2019 – see Finland's country report in the context of the European Semester.

Usefulness of SARs and false positives - sources: Europol and PWC



This results in deviation from the objective of detecting suspicious criminal activity and in a failure to implement the risk-based approach on which the AML/CFT framework is based. In many cases, only 1 in every 10 suspicions reported to the FIU is subject to an analysis shared with law enforcement authorities, although important divergences exist among FIUs based on the dissemination practices in place in each of them.

Feedback to other authorities is also insufficient. Every year, customs administrations receive around 100 000 cash declarations and detect around 12 000 cases where there was a failure to the obligation to declare cash above the threshold of EUR 10 000 when crossing of the EU external border. This information is reported to the FIUs but only seldom do customs administrations receive feedback. This is confirmed by the FIUs, but the very limited feedback is rather linked to an absence of obligation in the legal framework to provide any feedback on these reports to customs authorities. However, this feedback is particularly important in the case of infringements of the obligation to declare such sums. According to the above-mentioned Europol report, 38% of the suspicious transactions reported originate in cash-related data.

These three problems interact with one another to create a situation that continues to provide an economic lifeline for criminals. This allows them not only to jeopardise public security, but also to infiltrate the legal economy to obtain extra gains[25], with detrimental effects on welfare and public resources, including EU funds[26]. These weaknesses also impact the soundness and reputation of the EU's financial system, as some EU banks have had to terminate all or part of their business. From a broader economic perspective, as the International Monetary Fund notes, money laundering discourages foreign investment[27], which might in turn slow down the economic recovery following the COVID-19 pandemic.

At the same time, the current AML/CFT framework can impinge on the provision of services. Recent cases where financial institutions chose to de-risk by ceasing to offer certain services instead of managing the risks associated with certain sectors or customers have affected economic investments in some Member States[28] and, as noted by several stakeholders including the European Banking Federation, might also obstruct financial inclusion[29].

[25] See for example, Financial Times, *How the Mafia infiltrated Italy's hospitals and laundered the profits globally*, 8 July 2020.
[26] See for example, https://www.investigace.eu/italian-farms-slovak-soil/
[27] Factsheet - IMF and the Fight Against Money Laundering and the Financing of Terrorism, March 8, 2018
[28] https://www.rahandusministeerium.ee/en/news/martin-helme-fighting-money-laundering-must-be-smarter
[29] EBF blueprint 'Lifting the Spell of Dirty Money', March 2020

2.2 What are the problem drivers?

Three problem drivers are directly relevant for the initiatives to which this impact assessment relates, and are described in greater detail below.

2.2.1 Lack of clear and consistent rules

The current EU AML/CFT legislation centres around an anti-money laundering directive (AMLD), which provides a comprehensive regulatory environment to prevent and combat money laundering and terrorism financing. However, the lack of clarity, and limited nature, of some of the rules adopted at EU level, combined with different approaches in gold-plating, have resulted in diverging implementation of the EU legal framework across Member States and across obliged entities.

These divergences encompass a wide array of provisions. Regarding the scope, that is natural and legal persons that are subject to AML/CFT requirements, some have gone beyond the list in the Directive in different ways to cover crowdfunding platforms (Lithuania), the administrator of the emission trading registry (Czech Republic) or the administrator of the companies register (France). While in some cases specific risk situations might justify national divergences, the examples above are entities that share comparable risk levels across the EU, but which as a result of divergent approaches have not been consistently subjected to AML/CFT rules.

Unclear EU rules also lead to uncertainty as to how AML/CFT requirements must be applied by the private sector. This is exemplified in the report[30] investigating alleged money laundering through Swedbank's Baltic subsidiaries by Clifford Chance.

Example: Swedbank

Employee A: "[i]t is ludicrous to create separate KYC functions or banks in each Swedbank entity. It is not required by local law and is not required by the [supervisor, the] FSA (they would have said so if anyone would have bothered to ask them)."

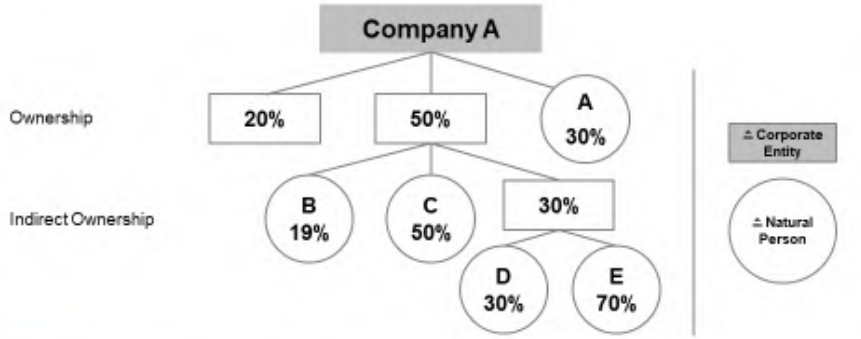
Employee B: "AML Manual is clear that our Baltic colleagues are requested by the local FSA to conduct their own KYC and independently come to a conclusion if they want to run a relationship or not."

Employee C: "[Swedbank and the Baltic subsidiaries] are separate legal entities and the relevant FSAs require a risk assessment of the customers by the relevant entity."

Further, the degree of transparency imposed by Member States regarding the beneficial ownership of companies and trusts often goes beyond the minimal requirements of the Directive, resulting in variation. While the majority of Member States have imposed a threshold of holding 25% of shares in a company to be entered into the register of beneficial owners, only two countries (Latvia and Spain) have opted for a lower

[30] https://internetbank.swedbank.se/ConditionsEarchive/download?bankid=1111&id=WEBDOC-PRODE57526786

threshold of 10% in order to enhance the transparency of corporate ownership.[31] Current rules are subject to divergent interpretations, and result in different methods to identify beneficial owners of a given legal entity due to inconsistent ways to calculate indirect ownership. Below is a graphic example that compares the rules in three different Member States[32].



Who is the ultimate beneficial owner of Company A?

	Germany (company law approach)	Italy („bottom up" approach)	Luxemburg („top down approach")
A	✓	✓	✓
B	x	x	x
C	(✓)[1)]	✓	x
D	x	✓	x
E	x	✓	x

[1)] should be considered risk based

As shown, the application of the relevant national rules leads to inconsistent results as to which person or persons are considered to be the beneficial owner(s) of the same legal entity. This creates serious problems in terms of transparency and hampers the ability to spot potential suspicions in one Member State as compared to another.

A further prominent case of inconsistent rules concerns the identification of obliged entities, with specific regard to the example of crowdfunding platforms, mentioned

[31] European Parliament - Policy Department A, *Improving Anti-Money Laundering Policy – Blacklisting, measures against letterbox companies, AML regulations and a European executive* (2020)
[32] Commerzbank, GM-CO Global Financial Crime Prevention, Frankfurt, June 2020.

above. Some national legal systems impose AML/CFT rules also to crowdfunding platforms, which are then subject to supervision and face specific requirements such as mandatory registration and transparency obligations. However, in the majority of Member States such entities are not supervised and regulated for AML/CFT purposes. This national approach is particularly inadequate considering that, as recognised by the Commission's 2019 Supranational Risk Assessment[33], crowdfunding platforms present risks and vulnerabilities that are horizontal and that affect the internal market as a whole. An inconsistent identification of such platforms is not justified by the presence of local risks that characterise only specific national realities, and leads to inability of the AML/CFT framework to monitor anonymous cross-border financial flows which are typical of such platforms.

The powers of national AML/CFT supervisors also vary significantly. The Bank of Italy (the AML/CFT supervisor for the financial sector in Italy) has the power to issue all ranges of administrative sanctions, and has gone beyond the sanctions towards natural persons set out in the AMLD (i.e. 5 million EUR), when the benefit is higher (sanction is at most twice the amount of the benefit obtained). On the other hand, Estonia is in the process of increasing the administrative sanctions that can be imposed by its financial supervisor, which are deemed too low. In the non-financial sector, the Irish Ministry of Justice can issue instructions to comply or revoke authorisations, but has no power to issue administrative sanctions. Similarly, the Danish supervisors of legal professions have no power to issue pecuniary sanctions on supervised professionals.

Similarly, not all FIUs share the same powers. Some FIUs, such as the Finnish and Greek FIUs, have been granted administrative powers to freeze assets for a certain period of time in view of a judicial freezing order in the context of a criminal investigation. While all FIUs have powers to issue requests for information to professionals subject to AML/CFT requirements, the timeframe for responding to such requests varies significantly across Member States, from 5 to 20 working days. Due to their varying status, not all FIUs are able to access directly and share swiftly all relevant information (financial, administrative and law enforcement information). Moreover, the 2016 Mapping exercise on FIUs' powers and obstacles to exchange and access information[34] and the 2019 Commission report assessing the framework for cooperation between FIUs[35] demonstrated that there are problems linked to the timeliness of replies to requests, as some FIUs indicate that they reply to requests from other FIUs within one month on average, which is far longer than the average time for exchange of information

[33] SWD(2019) 650 final
[34] This report is accessible on the website for the "Register Commission of expert groups and other similar entities" as an annex to the meeting minutes of the 31th meeting of the EU FIUs' Platform: http://ec.europa.eu/transparency/regexpert/.http://ec.europa.eu/transparency/regexpert/.
[35] COM(2019) 371 final

between authorities under other EU instruments[36] with detrimental effect on the effective use of such information and the adoption of measures where needed. EU law does not impose any deadlines for the exchange of information between FIUs.

In addition, current rules do not provide for an EU-wide interconnection of the centralised bank account registries. The 2019 Commission report[37] assessing the technical feasibility of such interconnection confirmed that this would be possible. These registries allow the identification of any natural or legal persons holding or controlling payments accounts, bank accounts and safe deposit boxes and as the 2019 report notes will be an important component in the fight against money laundering, associate predicate offences and terrorist financing. The lack of interconnection of centralised bank account registries hampers timely access to bank account information and cross-border cooperation among FIUs as well as AML/CFT competent authorities[38].

Finally, some Member States have taken measures to deal with the specific risks posed by cash by setting ceilings for large cash payments, whereas others have not. The 2019 SNRA concluded that the money laundering vulnerability of payments in cash is very high (the highest threat level). This is due to a number of facts, among which the large sums that can be engaged speedily and anonymously, including across borders, exposure across all sectors and low level of risk awareness. The current rules which provide for the application of AML/CFT measures to traders in goods for transactions of or above 10 000 EUR have not achieved the expected results. This is partly because of no framework/controls in place, or because enforcement of the controls is not efficient. Even where controls are in place, the transactions reported do not allow triggering a sufficient level of suspicion that would allow producing financial intelligence for the support of investigations.

EU rules are not only transposed and applied in a divergent manner, they are also not fully consistent with the latest international standards that have evolved since the latest amendment to the AMLD, as they fail to include all crypto assets service providers among the professionals who must apply AML/CFT requirements and are not adapted to the risks stemming from innovation. The lack of coherence with international standards also covers the traceability of the crypto assets transfers and the information sharing obligations between crypto assets services providers, as current EU rules, as laid down in Regulation (EU) 2015/847 only identified funds as "banknotes and coins, scriptural

[36] For example, Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union requires the Member States to have procedures in place enabling to respond to urgent requests for information and intelligence within at most 8 hours (Article 4).
[37] Report from the Commission to the European Parliament and the Council on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts, COM 2019(373) final.
[38] See annex 6 for more information on this subject.

money and electronic money", but not crypto assets. In their recent joint opinion,[39] the EU supervisory authorities identified specific risk-increasing factors in respect of new business models and products (i.e. fintech), first of which is the provision of unregulated financial products and services that do not fall within the scope of AML/CFT legislation.

Lack of clarity also exists in the interplay between AML/CFT rules and other sectoral legislation. The EBA recently identified the lack of explicit provisions regarding such interplay as a key source of the ineffective application of AML/CFT rules by supervisors and entities subject to AML/CFT supervision alike.[40] In its 2019 Opinion on deposit guarantee scheme pay-outs, the EBA identified gaps in the EU legal framework that have contributed to the adoption of divergent approaches by Member States to such pay-outs in situations where ML/TF concerns exist. Similarly, the lack of harmonised customer due diligence provisions has led to situations where Member States have transposed the Payment Account Directive and AML/CFT rules in a way that may prevent the application of a risk-based approach and result in denial of access to a basic payment account.

The consequence is an insufficient and ineffective application of AML/CFT obligations that fails to adequately prevent criminals from exploiting the EU's financial system to launder the proceeds of their illicit activities.

2.2.2 Inconsistent supervision across the internal market

AML/CFT supervision within the EU is currently Member State-based. Its quality and effectiveness are uneven, due to significant variations in resources and practices across Member States. In some cases, the variations cover the human and financial resources devoted to it. For example, only ten staff members are tasked with supervising compliance with AML/CFT rules by the financial sector in Finland as opposed to 27 staff members in Austria, despite financial sectors of a similar size and the presence in both countries of significant financial groups. In the non-financial sector, Belgium and the Netherlands allocated more than 10 staff members to the supervision of real estate professionals, whereas Croatia allocated 1 person to this task and Germany indicated having allocated 15 persons to the supervision of the whole non-financial sector (about 1 million entities).

As recent cases of alleged money laundering involving EU credit institutions show, the approach to cross-border situations is not consistent. The EBA's recent report on

[39] Joint opinion of the European supervisory authorities on the risks of money laundering and terrorist financing affecting the European Union's Financial Sector, 4 October 2019 (JC2019 59)

[40] https://eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Missions%20and%20tasks/Call%20for%20Advice/2020/883678/EBA%20Call%20for%20advice_AML%20Regulation_%20%28002%29.pdf

approaches of competent authorities to AML/CFT supervision[41] confirmed that despite progress, not all competent authorities are able to cooperate effectively with domestic and international stakeholders.

The methods to identify risks and to apply the risk-based approach to supervision also diverge. While some risks remain national in nature, others are of horizontal nature or may impact the entire Union financial system. Member States stressed the need for a common, consistent methodology to assess and identify risks in reply to the targeted questionnaire circulated by the Commission as part of the public consultation launched when adopting the Action Plan on 7 May 2020[42].

In addition to the divergences in supervisory powers already described, the EBA also notes that national AML/CFT supervisors might not always be willing to use the full set of powers available.

Excerpt from EBA report:

These challenges included translating theoretical knowledge of ML/TF risks into supervisory practice and risk-based supervisory strategies; shifting from a focus on testing compliance with a prescriptive set of AML/CFT requirements to assessing whether banks' AML/CFT systems and controls are effective, and taking proportionate and sufficiently dissuasive corrective measures if they are not.

This leads not only to inadequate supervision at national level, but also to insufficient supervision of professionals providing services across borders, which create risks for the whole Single Market.

2.2.3 Insufficient coordination and exchange of information among FIUs

FIUs serve as national centres for the receipt and analysis of suspicious transaction reports by the private sector and all cash-related data from customs administrations and other information relevant for the detection of money laundering and financing of terrorism. The results of such analyses should be consistently disseminated to other FIUs and competent authorities to investigate cases, inform supervisory activities and allow other measures (e.g. by tax authorities) to be taken.

Most FIUs have developed their own reporting templates and methods to identify suspicious activities and while a common template has been developed by the FIU Platform, it is not binding. As a result, the nature and extent of the information collected by FIUs is not always comparable.

[41] EBA/Rep/2020/06, available at https://eba.europa.eu/file/744071/download?token=Tf9XDqWX
[42] Not publicly available.

Even when the reports have a comparable content, the non-binding nature of the existing template results in a situation where not all EU FIUs use it. This makes the information contained in the report hardly recognisable or usable in timely manner by other FIUs, which hinders effective actions to identify and tackle potential cross-border money laundering or related predicate offences including tax crimes as well as terrorist financing activities. Performing joint analyses also becomes difficult when reports and the approach to analysing them differ substantially. Indeed, while 8 FIUs indicated using GoAML, a reporting system developed by the United Nations, 11 indicated that they have put in place their own reporting system, whether based on IT systems or analogic (e.g. fax). Similarly, when it comes to analysing these reports, 11 FIUs indicated that they do this without support from IT tools, 11 FIUs have an IT tool at their disposal to support the analysis, while only 4 FIUs indicated resorting to Artificial Intelligence (AI) tools (2 FIUs are in a testing phase).

Data shared by FIUs also reveals the absence of a common approach to data sharing. While almost all FIUs used the available tools such as FIU.net to disseminate reports, analyses or to request information, the use of more advance tools such as matching techniques was less widespread. The figures show significant variation in the amount of information exchanged. For example, FIU A shared 200 analysis, while FIU B shared 6. Behind the overall numbers, divergences exist in terms of what is shared (whether it is the report as submitted by the obliged entity itself or rather the analysis performed by the FIU) and when it is shared (e.g. automatically when the report contains a reference to a Member State or only when that report is relevant).

All recent major money laundering cases reported in the EU had a cross-border dimension. The detection of these financial movements is however left to the national FIUs and to cooperation among them. While this reflects the operational independence and autonomy of FIUs, the absence of a common structure to underpin this cooperation leads to situations where joint analyses are not performed for lack of common tools or resources. Indeed, only half of the FIUs indicated they use the current tools to build joint cases. Moreover, exchanges of practices and mutual learning remains marginal (only 5 FIUs reported having engaged in trainings with other FIUs), and in a number of cases FIUs have turned to the private sector to receive the kind of training that another FIU with experience in the field (e.g. trends in the misuse of corporate vehicles) would have been best placed to provide.

These divergences hamper cross-border cooperation, and thereby reduce the capacity to detect money laundering and terrorism financing early and effectively. This results in a fragmented approach that is exposed to misuse for money laundering and terrorist financing and that cannot timely identify trends and typologies at Union level.

2.3 How will the problem evolve?

Unless the EU adopts a new, comprehensive approach to preventing money laundering and terrorism financing that tackles the identified problem drivers, the EU economy and financial system will remain exposed to risks. While the current tools have gone a long way towards tackling these risks, they are not sufficient to address problems that due to a fast evolving context have become structural in nature.

Recent decisions by credit institutions to exit some markets and interrupt correspondent banking services provide an indication that any failure to act at EU level to ensure consistent application of the rules might have negative effects on legitimate business. At the same time, there is no indication that de-risking brings benefits in terms of preventing money laundering or terrorist financing, as laundering techniques continuously evolve. The private sector often lacks information on new trends to apply a smart approach that could differentiate suspicious activities from legitimate ones.

As Europol notes, money laundering risks are likely to increase during the recovery from the COVID-19 pandemic. The volatile economic situation will make the EU financial system, as well as sectors such as real estate and cash-intensive businesses, particularly exposed. In the longer term, laundering techniques are likely to become more sophisticated and involve an increase in the use of shell companies, trusts and trade-based money laundering.[43] Without a consistent response by the private sector, supported by adequate supervision, the EU AML/CFT framework will be unlikely to resist such attempts. This presupposes an understanding of the risks, which the current level of feedback by FIUs and cooperation among all authorities cannot grant.

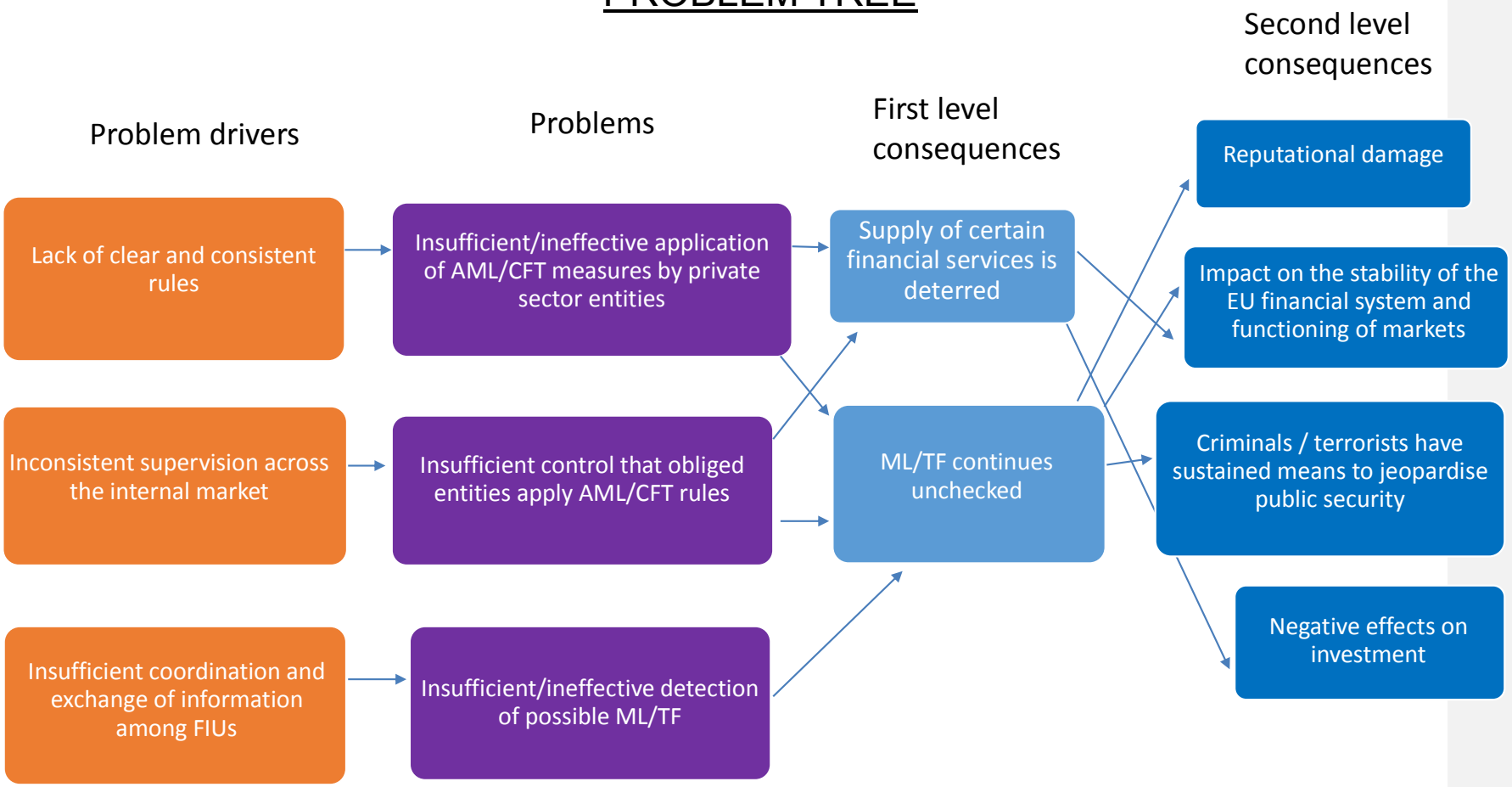
New threats accompanying innovation in financial services will also appear. As Europol notes, "[a] growing number of online platforms and applications offer new ways of transferring money and are not always regulated to the same degree as traditional financial service providers. This makes money laundering a technical challenge for law enforcement authorities to investigate"[44]. In the absence of specific obligations on providers of such services to apply AML/CFT measures and to report any suspicious transactions or activity, criminals will continue laundering their illegal proceeds through these systems undetected.

For these reasons, the AML/CFT legislative framework will need periodic updating and amendment, at least as regards the scope of Obliged Entities which are covered, and possibly other aspects of rules. Such updating can be facilitated by certain elements of the selected options described in sections 6 and 7 below, including directly applicable

[43] Europol, *Beyond the pandemic - How COVID-19 will shape the serious and organised crime landscape in the EU* (2020)
[44] Europol, *Enterprising criminals - Europe's fight against the global networks of financial and economic crime* (2020)

key rules and the existence of an EU AML/CFT Authority which can provide analyses and guidance on an ongoing basis. It is however anticipated that the basic institutional and legislative framework provided by the present package of proposals, if not always the detailed rules, will be "future proof" in the face of evolution in the practices of money launderers and financers of terrorism.

PROBLEM TREE



3 WHY SHOULD THE EU ACT?

3.1 Legal basis

The legal basis of most parts of this the initiative, like previous initiatives in the area of AML/CFT, will be Article 114 TFEU, which allows the legislator to adopt rules in order to achieve the objectives announced in Article 26 TFEU and aims at ensuring the proper functioning of the Internal Market. Article 114 TFEU provides a legal basis for the approximation of national laws with the final objective of ensuring the proper functioning of the internal market. As held by the Court in its judgement in Case C 58/08 Vodafone and others, the resort to Article 114 TFEU is justified where there are differences between national rules which have a direct effect on the functioning of the internal market. Equally, the Court held, that where an act based on Article 114 TFEU has already removed any obstacle to trade in the area that it harmonises, the Union legislature cannot be denied the possibility of adapting that act to any change in circumstances or development of knowledge having regard to its task of safeguarding the general interests recognised by the Treaty.

The situation as presented in the problem definition confirms that these divergences are actual and current and have a direct effect on the functioning of the internal market and experience with the current AMLD framework has shown weaknesses that justify being addressed. This justifies the adoption of clearer rules to avoid such differences. Similarly, the development of national AML/CFT laws aimed at integrating international recommendations in relation to crypto assets is likely to lead to the emergence of new obstacles to trade, which the Court also held as justifying the adoption of measures under Article 114 TFEU. EU action is needed to prevent the emergence of such new obstacles and the proposed measures must be designed to do so.

Finally, the Court held that the measures for the approximation covered by Article 114 TFEU are intended to allow a margin of discretion, depending on the general context and the specific circumstances of the matter to be harmonised, as to the method of approximation most appropriate to achieve the desired result. As explained in the problem definition, the existing issues are of a structural nature and require measures that aim at introducing EU-level structures in support of national ones.

In light of the above, and in respect of the jurisprudence of the Court, the aim of this initiative is to provide a harmonised approach to strengthening, taking into account experience, the EU's existing AML/CFT preventive framework by reducing divergences in national legislation and by introducing structures that would deliver a real harmonization effect, thus allowing effective implementation of the framework.

As noted in Annex VII, the extension of access to interconnected bank account registers to law enforcement authorities will have to have as legal base article 87(2) of the Treaty, the same legal basis as for Directive 1153/2019, which extended access to domestic bank account registers to national law enforcement authorities[45]. That is the only element of the present package concerning law enforcement as opposed to upstream prevention or detection of money laundering and terrorist financing.

3.2 Subsidiarity: Necessity of EU action

The current fragmentation of rules and their implementation framework has resulted in weak links in the EU anti-money laundering framework. The alleged money laundering cases that involved EU credit institutions and professionals since 2018 show significant cross-border dimensions that cannot be sufficiently addressed though the minimum harmonisation provided by AMLD.

As the previous section shows, the issues are of a structural nature and cannot be remedied by Member States acting alone. An ineffective AML/CFT framework in one Member State or differences between rules across Member States, may be exploited by criminals and have consequences for other Member States. Member States alone cannot ensure consistent integration of the latest international standards in the EU framework, nor increased consistency with other EU rules to the extent needed to solve the problems identified.

Member States acting alone are also not able to ensure the consistency of rules and their supervision across the EU. This affects the capacity of Member States to protect the integrity of the internal market, but also the ability of companies to operate freely or for customers to easily contract financial services across borders.

Action by Member States alone is not sufficient to ensure effective coordination and exchange of information among FIUs to identify cross-border transactions and activities that are susceptible to be connected to money laundering and terrorist financing.

It is therefore important to act at EU level. This has been recognised in the five previous iterations of the AML Directive, and is still the case as regards this legislative package.

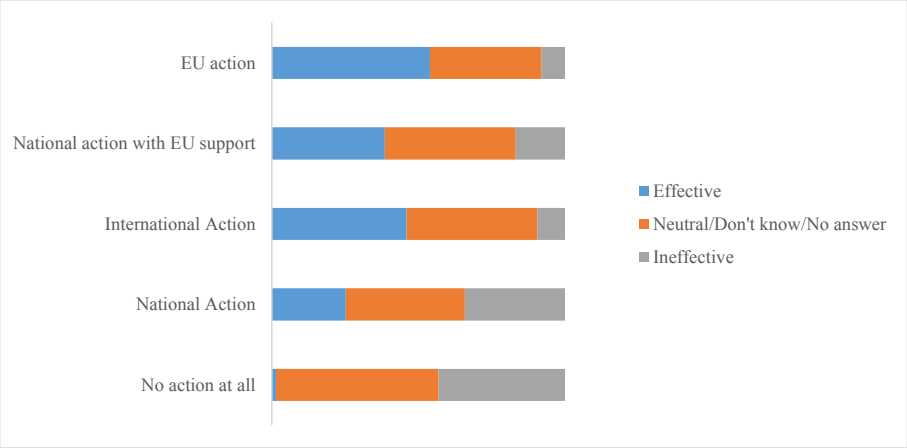
3.3 Subsidiarity: Added value of EU action

The actions needed to address the problems set out in chapter 2 can be better implemented at Union level. This would improve the robustness of the EU's AML/CFT framework and help reduce the fragmentation of measures taken to address money laundering and terrorism financing risks. It would also avoid implementation of unilateral measures and conflicts in legislation between Member States, in line with the objective of Article 114 TFEU and existing case law.

[45] See footnote 116 below.

It would also ensure a more effective and coherent implementation and enforcement. Individual national solutions are likely to lead to conflicting outcomes when confronted with the free movement of capital inherent to the internal market. A multiplication of national rules would also make it disproportionately difficult for professionals to provide services across borders.

The replies provided to the public consultation confirm that EU action in this area is likely to deliver better outcomes than Member States action in that it would deliver a real harmonization effect to close the loopholes that currently expose the EU's financial system and economy to money laundering and terrorist financing. Of all options available for taking further steps to fight money laundering and terrorist financing, respondents considered that action at EU level was likely to be the most effective, and also the least likely to be ineffective.



4 OBJECTIVES: WHAT IS TO BE ACHIEVED?

4.1 General objectives

The general objective is to achieve a comprehensive AML/CFT framework that will adequately protect the EU's economy and financial system from criminal infiltrations, as well as to ensure public security. Such a framework should be flexible enough to adapt to the evolving nature of the threats, risks and vulnerabilities facing the EU. It should approach risk in a smart manner to reduce negative effects on economic activity or citizens' right to privacy and protection of personal data to what is absolutely necessary and proportionate.

4.2 Specific objectives

This general objective translates into three specific objectives:

- Strengthen EU anti-money laundering rules and enhance their clarity while ensuring consistency with international standards and other EU legislation;
- Improve the effectiveness and consistency of anti-money laundering supervision, and
- Increase the level of cooperation and exchange of information among Financial Intelligence Units.

5 WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1 What is the baseline from which options are assessed?

The baseline scenario coincides with the first pillar of the Commission's Action Plan effective application of existing rules, i.e. the EU anti-money laundering framework consisting of the current Directive and the Wire Transfer Regulation[46]. The former would be transposed by Member States, with possible significant delays. The Commission would monitor such transposition and would open infringement proceedings in case of incomplete or incorrect transposition. However, the Commission would have no power to reduce divergences among Member States. The rules would indeed remain subject to broad margins of interpretation by Member States, due to the lack of detail. Thus, the fragmented application of EU rules and divergent national standards would persist. The Commission would use the European Semester exercise to identify situations where the effectiveness of national anti-money laundering frameworks needs improving, but would only be able to propose non-binding recommendations. The current inconsistencies between anti-money laundering rules and other EU legislation would continue to exist.

Supervision would continue to be fragmented, with national competent authorities solely responsible for ensuring compliance with AML requirements by private sector entities within their national jurisdictions. For entities that operate on a cross-border basis, multiple supervisory authorities would remain involved in supervision, based on a strict home-host distribution of supervisory responsibilities. The European Banking Authority would continue to perform a coordinating role. In the financial sector, EBA would continue to fulfil its current mandate in the area of AML/CFT, specifically with regard to: 1) harmonisation of the regulatory requirements for supervisory policy approaches by means of issuing binding technical standards, guidelines and recommendations; 2) promoting convergence in supervision by, inter alia, conducting peer and staff reviews of national competent authorities; 3) facilitating cooperation and information exchange between national competent authorities by establishing and hosting a data hub and participating on the work of AML colleges; 4) contributing to effective enforcement of Union law using all the tools at its disposal for that purpose, including, where necessary, breach of Union law powers[47]. However, EBA's governance structure might make it

[46] Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds.
[47] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Banking Authority, as amended by Regulation (EU) 2019/2175, enhancing the powers of EBA in the area of AML/CFT.

difficult to take action against a national supervisor which is ineffective in enforcing the rules.

The FIUs would continue to provide advice and expertise to the Commission on operational issues, and to exchange information on cooperation-related issues in the context of the current informal EU FIUs' Platform. However, matters pertaining to international cooperation, the identification of suspicious transactions with cross-border dimension, the use of IT tools such as the FIU.net system[48] and the adoption of common templates or performance of joint analyses would be on an individual, voluntary basis. Trends in money laundering and terrorist financing would also be discussed, but there would be no tool available to go beyond exchanges of views and of information. Thus, the current shortcomings of the framework for exchange of information and cooperation between FIUs would continue to exist and affect negatively their ability to detect and prevent money laundering and the financing of terrorism.

5.2 Description of the policy options

5.2.1 Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards

Option 1: EU rules would remain as they are with no modifications

Option 1 would constitute the baseline scenario described above in Section 5.1.

Option 2: Ensure a greater level of harmonisation in the rules that apply to obliged entities and leave it to Member States to detail the powers and obligations of competent authorities

Under this option, a number elements of the current framework that apply to entities subject to AML/CFT obligations would be made more consistent across the EU by more detailed rules, in a directly-applicable Regulation, while remaining in a minimum harmonisation system which allows Member States to go beyond. The logic of such an intervention is to carry out a structural reform of the rules with the aim to reduce the margins of interpretation that Member States have today. This would be achieved by detailing the current rules in a coherent way across the EU. This reform would address needs that are different in nature from those that led to the 5th AMLD. The latter, indeed, was adopted for the purpose of updating the framework in view of the FATF standards and to go beyond them (however, since then new FATF standards regarding CASPs have been adopted, which need to be incorporated into the EU framework). On the contrary, under option 2 and 3 (see below), this reform would not seek to introduce major new rules, but essentially to restructure and detail the current ones to ensure a coherent implementation across the EU.

[48] FIU.net is a secure infrastructure for exchange of information between FIUs. Hosting of FIU.net will be temporarily transferred to the Commission (where it will be hosted in DG OLAF) following a decision of the European Data Protection Supervisor that Europol, the current host, may not treat personal data of persons other than suspects. [EDPS decision of 19 December 2019].

Under Option 2, as stated above, this harmonisation would not concern all the current rules, but only key elements of those applicable to obliged entities. One example of such an element is the measures related to customer due diligence (CDD). In this regard, a homogeneous approach would be ensured in required procedures to identify and verify customers and beneficial owners, as well as in relation to the monitoring of transactions and business relationships and the related reporting obligations in case of suspicion. Harmonisation would also concern simplified and enhanced CDD measures to be adopted in lower/higher risk scenarios. This would include an adapted policy towards third countries to bring about a greater degree of granularity in definition of mitigating measures[49]. Further, this option would cover rules applicable to reliance on third parties for the performance of CDD and to internal controls that entities subject to AML/CFT controls must have in place, including data protection requirements. Provisions regulating the use of digital identities for digital customer identification and verification would also be included. Such rules, however, could still be sufficiently flexible for the specific purpose of accommodating a risk-based approach at the level of obliged entities, in line with international standards, and leaving scope for adopting specific rules to go further, with a high level of granularity. This could be achieved through regulatory technical standards to be developed by the EU AML Authority (see discussion of other problems).

Also, under this option a consistent approach would be introduced to the beneficial ownership (BO) transparency regime. This would include making sure that the same information is collected on beneficial owners of legal entities and legal arrangements across the EU, and that the same parameters are used for the definition of beneficial ownership. Moreover, consistent rules on the collection and storing of BO information in central registers would be put in place.

This option would also include interconnection of bank account registers for AML/CFT authorities, as discussed in more detail in Annex 7, which considers the main policy options available, i.e. interconnection of the bank account registers and access to them by FIUs only or interconnection of the bank account registers and access by FIUs as well as other competent authorities, namely those covered by Directive (EU) 2019/1153. Options regarding the introduction of limits to large cash transactions are discussed in more detail in Annex 9. Those are: keeping the status quo by relying on traders in goods while allowing Member States to define stricter rules, introduce an upper EU-wide limit for large cash payments while allowing Member States to adopt stricter limits at national level or introducing an EU-wide harmonised limit to large cash payments.

Furthermore, this option would entail the adoption of a more harmonised list of obliged entities across all Member States. In line with the risk-based approach that lies at the basis of the AML/CFT system, the new rules would also provide a mechanism to allow Member States to add other entities, if evidence shows this is necessary in order to address specific risks at national level. This option would also address the relationship with other EU laws interacting with AML rules (see section 7.3 below).

[49] More detail about the approach to third countries is provided in annex 8.

Among the obliged entities to be added, in addition to crowdfunding platforms (see annex 6), there is the need to introduce important categories of crypto assets services providers recently covered by the FATF standards. FATF also recommends to introduce harmonised EU processes to share information on crypto assets transfers, both between crypto assets services providers at the two ends of such transfers (beneficiary and originator crypto assets services providers), but also by keeping this information available for competent authorities.

These are the main areas for greater harmonisation; Annex 6 discusses in more detail all the areas proposed for improved harmonisation.

Areas proposed for a greater level of harmonisation under option 2

- Customer Due Diligence (CDD) ;
- list of obliged entities;
- beneficial ownership transparency regime;
- central registers for bank accounts – providing the legal basis for the interconnection at Union level;
- Limits to large cash transactions
- AML/CFT systems and controls, including governance arrangements;
- Suspicious Transaction Reporting;
- occasional transactions;

Option 3: Ensure a greater level of harmonisation in the rules that apply to entities subject to AML/CFT obligations and the powers and obligations of supervisors and FIUs

This option would include the elements covered by option 2 and, in addition, it would provide for greater consistency also with regard to the powers and obligations of AML/CFT supervisors and Financial Intelligence Units. The legislative proposal would lay down minimum common rules covering the performance of key supervisory tasks such as the risk categorisation of obliged entities, the obligation to perform sectorial risk assessments, minimum rules for on-site supervisions, as well as minimum powers that AML supervisors should have. The rules would also cover operational aspects of cooperation among national AML supervisors, as well as the cooperation with a possible EU AML supervisor, if appropriate (see section 5.2.2. below. Consistency across the EU would also be introduced concerning the circumstances, the criteria and the thresholds for application of administrative sanctions by supervisors towards obliged entities in case of breach of AML/CFT obligations. Furthermore, an obligation would be introduced in line with FATF standards to ensure that when AML supervision is performed by self-regulatory bodies such as bar associations, they are themselves subject to supervision by a public authority. As regards FIUs, this option would involve defining their core tasks in relation to the production and dissemination of financial intelligence and a minimum set of powers (e.g. powers to freeze a transaction). Moreover, this option would allow

enhanced cooperation with other competent authorities such as customs and tax authorities (for example, FIUs could be obliged to share with tax authorities information about large undeclared cash movements into the EU).

Areas proposed for a greater level of harmonisation under option 3 (more details in annexes 6, 7 and 9)

- Customer Due Diligence (CDD) ;
- list of obliged entities;
- beneficial ownership transparency regime;
- AML/CFT systems and controls, including governance arrangements;
- Suspicious Transaction Reporting;
- occasional transactions;
- tasks and powers of supervisors and FIUs;
- operational cooperation between relevant national competent authorities;
- administrative sanctions – criteria and thresholds;
- central registers for bank accounts – providing the legal basis for the interconnection at Union level;
- limits to large cash transactions.

5.2.2 Improve the effectiveness and consistency of anti-money laundering supervision

Option 1: Anti-money laundering supervision would continue to be performed at national level, with the European Banking Authority in charge of overseeing this supervision in the financial sector

Option 1 would constitute the baseline scenario described above in Section 5.1.

Option 2: Establish indirect oversight over all obliged entities

Similarly to the baseline scenario, under this option AML supervision in the Union would remain primarily at national level, with national competent authorities retaining full responsibility and accountability for direct supervision of obliged entities. This model would build on the AML mandate currently carried out by EBA but strengthen it further with respect to both competences and powers. At EU level, an AML Authority would be granted adequate powers to ensure that supervisory actions at national level are consistent and of a high quality across the EU.

For this, the EU AML Authority would need to have extensive access to real time information from national supervisors about their activity, and this access could be used

to identify and communicate trends and risks, conduct more targeted reviews of national supervisory approaches, and foster information exchange and cooperation. Through its indirect oversight capacity, the AML Authority would contribute to enhancing supervisory convergence, cooperation and information exchange between national competent authorities.

The scope of the activity of this Authority would expand to cover the non-financial sector, where it would facilitate convergence of supervisory practices, exchanges of good practices and peer reviews. In specific cases where national supervision is insufficient, it would be given powers to recommend specific actions to the national supervisors.

Option 3: Direct supervisory powers over selected risky entities in the financial sector subject to AML/CFT requirements and indirect oversight over all other entities

This option would go beyond the previous option by providing a capacity of direct supervision of a selected number of entities at EU level to an EU-level supervisor in the form of a decentralised agency[50], based on objective criteria concerning their risk-level and cross-border nature, as laid down in a risk matrix to be developed by the Authority and adopted by the Commission as a delegated act. The criteria will be such that the entities in question would be mostly, or entirely, cross-border financial groups, at least in an initial period[51]. Entities subject to direct supervision at EU level would be selected periodically given their shifting residual risk profile, and the objective criteria for their selection would be established in Union law. In order to ensure that Member State-specific risks are nevertheless appropriately understood and addressed, EU level supervision would be carried out with full involvement of all relevant national authorities in day-to-day supervision in cooperation with the staff of the EU AML authority, leaving the overall responsibility and accountability for all the binding decisions taken towards the supervised entities to the EU AML supervisor.

The vast majority of the financial sector obliged entities would remain under the direct supervision of national authorities, while indirect supervision of the activities of the national supervisors as described in option 2 would ensure a sufficient degree of convergence of supervisory approaches towards such entities. In cases where serious ML/TF risks at particular supervised entities are not appropriately or in a timely manner addressed by the respective national supervisory authority, the EU AML supervisor would have the powers to take over the supervision of specific entities, based on a procedure laid down in EU law[52]. This could be done for any financial institution, independently of risk profile or cross-border activity, as it would be based on the identification of specific, rather than potential conditions (e.g. material breaches of rules,

[50] See annex 6 for a discussion of whether a new body should be created for that purpose (a decentralised Agency), or whether the existing EBA should receive that task.
[51] The current implementation of supervision in the non-financial sector, and the very fragmented landscape in the regulation of these sectors would raise significant challenges and reduced benefits for EU-level supervision at present. Nevertheless, possible extension of EU-level supervision to the riskiest entities in such sectors is not ruled out in the longer term.
[52] The European Commission would confirm such a transfer of supervisory competence via a legal act.

request by national supervisor). The role of the EU Authority over non-financial sector supervisors would be as under option 2, with oversight and coordination of national supervisors.

Option 4: Direct EU-level anti-money laundering supervision of all obliged entities

This option, like option 3, would require establishing an EU-level supervisor with direct powers over entities subject to AML/CFT obligations. Under this option, however, the scope of entities to be supervised by this entity would be much broader, and so would the resources needed to deliver on its tasks. The supervision would be based on fully harmonised rules and powers of the Union level supervisory authority. Therefore, this option could only be executed in conjunction with option 3 relating to harmonisation of substantive rules, as described above.

Under this option, a Union-level supervisory authority would be responsible and accountable for taking all binding decisions and imposing administrative measures and sanctions towards all the obliged entities in the Union.

5.2.3 Increase the level of cooperation and exchange of information among Financial Intelligence Units

Option 1: Financial intelligence units would continue to cooperate in the context of the EU FIUs' Platform, which would be classed as a network

Option 1 would constitute the baseline scenario described above in Section 5.1.

Option 2: Transform the EU FIUs' Platform into a comitology committee leaving it to the Commission to adopt implementing acts defining standards for FIUs

Under this option, as in the baseline scenario, the EU FIUs' platform would provide the main framework for cooperation among FIUs. This option, however, entails the transformation of the EU FIUs' Platform into a comitology committee. The Commission would be granted implementing powers to define standards relevant for the work of the FIUs, e.g. as regards reporting of suspicious transactions.

This option would allow to impose common templates, harmonisation of terminology and procedures for exchange of information between FIUs and possibly to facilitate further introduction of Artificial Intelligence (AI) tools through standardisation of data processing.

Option 3: The EU FIUs' Platform would become an EU mechanism with power to issue guidelines and technical standards and to organise joint analyses and training, carry out trends and risks analysis (legislative action)

This option would see the EU FIUs' Platform become a formal coordination mechanism of EU FIUs, in principle part of the same Authority in charge of supervision (see section 5.2.2. above), but with its own budget allocation and own operational staff. The

governance of the combined agency would ensure that EU FIUs are responsible in decision-making when FIU issues are concerned.

In contrast with the previous option, its financial and human resources would enable the mechanism to centrally coordinate at strategic level joint analyses of intelligence produced by national FIUs and identify Union-wide risks and trends, without having access to the content of suspicious activity or person. In addition, it could offer training programs and capacity building, provide support services for FIUs such as IT services for information sharing necessary for carrying out joint analyses and disseminating information as well as support in the use of AI tools, whilst maintaining the same approach to the treatment of personal data, which at operational level would remain solely with the FIU having received them.

The AML Authority would receive own regulatory powers and be able to approve draft binding technical standards regarding templates, and also non-binding guidance, addressed to the FIUs or to obliged entities. The national FIUs would be fully involved, through the mechanism, in the development of these standards, which would be submitted to the Commission for adoption as Regulatory Technical Standards.

The Authority could also play a role of mediator between FIUs in cases of differing views or alleged inadequate compliance with the AML legal framework, including binding acts. While respecting the principles of independence and autonomy of FIUs, peer reviews could also be organised, with assessment drawn up by other FIUs.

Option 4: The EU FIUs' Platform would become an EU-level FIU, replacing national FIUs

The setting-up of an EU–level FIU would consider the Union as a single jurisdiction for AML/CFT purposes and in relation to international standards in this area. This could be justifiable given the cross-border nature of money laundering and terrorism financing, and the shortcomings identified in the exchange of information between FIUs (see section 2.2.3). These shortcomings are due notably to the lack of i) resources allocated by jurisdictions to their FIUs, (including IT tools in particular for mass data handling and joint analysis projects) ; ii) a comparable range of data available to or accessible by each FIU, and iii) common understanding of the level of "analysis function".

In this scenario, an EU-level FIU would replace national FIUs and would be competent for receiving reports of suspicious transactions directly from all the obliged entities in the Union. In order to perform its tasks, the EU-level FIU would need to get sufficient human resources amounting to at least the sum of resources available to all national FIUs. Whilst such EU-level FIU would seem able to put in place powerful IT and AI tools to analyse data, direct access to national data and EU interconnected registers, or access to such data through national competent authorities, would be needed to produce financial intelligence of adequate quality, as well as powers to interact and cooperate with national law enforcement agencies.

6 WHAT ARE THE IMPACTS OF THE POLICY OPTIONS AND HOW DO THEY COMPARE?

6.1 Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards

Under the baseline scenario, the EU anti-money laundering framework would continue to be characterised by the minimum level of consistency ensured by the current rules. However, the current framework, as described above, falls short of providing an effective response to the ML/TF risks, especially in the context of improving the functioning of the internal market. More specifically, the rules applicable to the entities subject to AML/CFT obligations would continue to be subject to diverging and inconsistent implementation across the EU, partly due to the setting of requirements that go beyond those laid down in the Directive. The CDD rules that obliged entities have to apply would continue to differ from one Member State to another, depending on the prescriptiveness of the adopted approach. Moreover, the conditions that trigger the obligation to apply CDD would not be the same across the EU, therefore, if the same situation arises in different Member States, entities could potentially be required to either apply or not to apply CDD depending on where they are located. The same would apply to the conditions and the rules regarding simplified CDD and enhanced CDD. Such variation generates legal uncertainty and entails a significant compliance burden for entities subject to AML/CFT rules that operate cross-border, with adverse impacts on their capacity to detect suspicious transactions.

In addition, the baseline scenario would be insufficient to secure consistent levels of transparency across the EU, given that current EU rules result in Member States introducing different criteria for the identification of beneficial owners. The fragmentation of the legislative landscape that results from the baseline scenario is further exacerbated by the inconsistent designation of entities subject to AML/CFT obligations, as some Member States go beyond the EU law requirements and include entities that are not covered in other Member States. This scenario leads to an uneven playing field and a fragmentation with potential for regulatory arbitrage, and which makes the AML/CFT framework more vulnerable to ML/TF risks.

The lack of detail in the current rules also leads to divergences in the approach to supervision and in the assessment of ML/TF risks. The methodologies to assess such risks vary in quality and scope, thereby producing different and inconsistent outcomes across the EU when supervisors in different Member States deal with similar situations. This also hampers their ability to develop a common understanding of risks across the EU, with consequences also in terms of adequate and consistent supervision. This constitutes a serious obstacle to effective action in the context of cross-border cases, which require a consistent approach and fruitful cooperation. In addition, the current framework leads to a fragmented approach when it comes to holding obliged entities accountable in case of breach of the AML/CFT obligations. The findings of the

Commission's Report on trusts and similar legal arrangements[53] provide an example of this, showing an inconsistent identification of legal arrangements similar to trusts by Member States and an uneven imposition of the AMLD obligations with respect to them. A similar situation can be witnessed in relation to the exemptions that certain Member States grant to providers of gambling services[54]. Moreover, on the same line, the rules are not clear about what constitutes a proportionate and dissuasive sanction. The lack of clarity in the powers that supervisors should have results in a variation of approaches to similar situations, and hampers supervisors' ability to ensure that AML/CFT rules are applied consistently across the EU.

Under Option 2, the legislative proposals would allow the creation of a more level playing field across the EU as regards rules and obligations applicable to obliged entities. Compared to the baseline scenario, such entities would have to apply the same and consistent set of CDD measures defined at EU level, under the same circumstances and using the same criteria, regardless of where they operate in the EU. This would also better cover transactions involving crypto-assets. Such rules, however, could still be sufficiently flexible for the specific purpose of accommodating a risk-based approach at national level, leaving some scope for national rules going further. This would considerably enhance legal certainty and reduce compliance costs (at least for cross-border entities), facilitating cross-border transactions as well as the detection of suspicious activities across the EU. Under this option, obliged entities would face clearer and more consistent rules as regards the internal systems and controls that they have to set up in order to operate in the EU. In addition, the criteria for the identification of beneficial owners (BOs) of legal entities and legal arrangements would be established at EU level, so that obliged entities would be able to identify BOs in a consistent way regardless of where they operate, with significant improvements in terms of transparency and thereby eliminating the risk of regulatory arbitrage.

Compared to the baseline scenario, this option would thus remove the fragmentation deriving from different interpretations and implementation of EU rules on such matters, allowing for an identification and verification of customer identity, including beneficial ownership, which is consistent across the EU. A similar result would be achieved with regard to the list of obliged entities, which would be defined at EU level. In this case, Member States wishing to go beyond the EU rules and identify additional entities would have to provide adequate justification, which would allow an assessment of whether the risks are national only or rather of a supra-national scope. Such a consistent approach would ensure legal certainty on the status of certain service providers with regard to the list of obliged entities and would make sure that the same sectors are subject to consistent AML/CFT requirements across the EU. Moreover, compared to the baseline scenario,

[53] Report from the Commission to the European Parliament and the Council assessing whether Member States have duly identified and made subject to the obligations of Directive (EU) 2015/849 all trusts and similar legal arrangements governed under their laws, COM(2020) 560, 16.9.2020.

[54] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1602835953439&uri=CELEX:52020XC0731(01)

under this option the provisions in relevant sectorial legislation would be reconciled with AML/CFT rules, thus providing certainty to market operators, especially in the financial sector, regarding the AML/CFT implications when applying certain EU rules such as those related to payment services, e-money or wire transfers operations. This option would also address the challenges posed by digitalisation, by providing a strengthened and clear set of rules for private entities to regulate remote customer identification and verification in a consistent way across the Member States.

A consistent approach to the rules applicable to obliged entities would significantly facilitate cross-border business activities by such entities by reducing the cost of dealing with divergent AML/CFT frameworks. As a result of the current fragmentation, entities that operate cross-border are forced to adapt to divergent national rules and standards when it comes to carrying out key activities such as identifying and verifying customers and beneficial owners, thus facing uncertainty and high compliance costs. Cross-border crime should be tackled with more harmonised rules that apply consistently across the EU, thus creating a level playing field. This would also significantly contribute to removing barriers to business activities in the internal market. For example, entities subject to AML/CFT obligations would have to apply the comparable CDD measures under the same circumstances regardless of where they operate. The identification and verification of customers and beneficial owners would follow the same parameters and criteria across the EU. As a result, such entities would be able to significantly reduce the costs needed to adapt their internal systems and control procedures to the different national frameworks. Clear and detailed rules applicable consistently throughout the EU would also ultimately improve the entities' capacity to monitor relevant transactions and thus the effectiveness of the EU AML/CFT framework.

A clearer approach to Customer Due Diligence, combined with the refined approach to transactions involving third countries described in annex 8, should give Obliged Entities more confidence to offer services which they currently withhold out of caution and fear of unwitting breaking of rules, and also reduce the current element of overnotification of possible suspicious transactions to FIUs, which generates a high proportion of "false positives", and hinders FIUs in their work.

However, under this option rules applying to competent authorities concerning issues such as cooperation, supervisory approaches and ML/TF risk assessment would continue to be defined at national level. On these matters, option 2 would not change the baseline scenario already described. This would create a mismatch, as consistent rules for obliged entities would be complemented by fragmented and inconsistent rules about their enforcement. This might not eliminate the issues witnessed in some recent cases and described in the "post-mortem report", where local approaches undermined the application of stricter, more developed, AML/CFT measures, and might therefore undermine the efforts to raise standards applied by the entities subject to AML/CFT rules. Cross-border business relationships would still be difficult to monitor, as current rules on cooperation are vague and insufficient to ensure consistent approaches and procedures by FIUs and supervisors in different Member States, and the risk assessment

would not be homogeneous. If a level playing field and enhanced legal certainty for entities would facilitate compliance and detection of cross-border suspicious activities, insufficient cooperation and inconsistent understanding of risks by competent authorities would risk jeopardizing the benefits of such a consistent approach.

The lack of consistent supervisory powers has also led to supervisors not having the same capacity to compel the provision of relevant information and to impose administrative measures and sanctions to supervised entities. As regards FIUs, insufficiently detailed rules have caused poor cooperation and information exchange, fuelled by the fact that the methods to assess risks and information about suspicious activities are inconsistent across Member States. Unless the EU AML/CFT framework provides for a minimum set of powers and for more detailed duties to cooperate for supervisors and FIUs, the AML/CFT system cannot achieve a level of effectiveness that is appropriate to tackle AML/CFT threats. For this reason, even if the rules applicable to obliged entities are consistent, the presence of weak supervisory links in the EU causes a risk of regulatory shopping and impairs the effectiveness of the whole system, especially with regard to cross-border cases.

Under option 3, rules applicable to the activity of competent authorities, in particular the methodologies and procedures to be applied, their powers and modalities for their cooperation between one another and with other competent authorities, would be clearly defined at EU level and would not be subject to divergent interpretation and implementation by Member States. Compared to option 2, supervisors would have to assess ML/TF risks by applying the same and consistent methodology across the EU, using the same criteria and parameters. This would allow for a comparable assessment of risks related to specific sectors, entities and business relationships, thus allowing for a consistent supervisory response in all Member States. National competent authorities would have more detailed rules regarding the obligation and modalities to cooperate and to exchange information, both at national level and in the context of cross-border cases. From this viewpoint, EU rules would ensure that, when dealing with cross-border situations, respective national authorities have clear responsibilities, as well as legal duties to apply homogeneous procedures that ensure a fully-fledged cooperation and an effective monitoring of cross-border transactions. A consistent approach at EU level to such rules would remove uncertainties deriving from divergent implementation and would allow for an effective response to ML/TF threats, regardless of where they arise in the EU. In addition, under option 3, binding rules fixed at EU level would make sure that national supervisors cooperate effectively with a possible EU-level supervisor (see below), in order to avoid that EU-level supervision is impaired by inconsistent and lengthy procedures when supervisory action requires joint efforts at EU and national level.

Moreover, compared to option 2, under option 3 the EU law would set out the minimum set of powers that supervisors should have, and criteria for determining the seriousness of breaches of AML/CFT obligations by entities subject to them, as well as the most appropriate supervisory responses, including sanctions and corrective measures. Under

this option, therefore, also such criteria could not be subject to diverging interpretations at national level. Option 3 is also a prerequisite for any direct supervision at EU level of certain entities by an EU supervisor, and will greatly facilitate coordination of national supervisors by an EU supervisor.

By introducing a consistent and more granular approach to the above rules at EU level, option 3 would allow to remove the current fragmentation both as regards AML/CFT obligations for obliged entities, and the activities of competent authorities. This way, the level-playing field that would be achieved under option 2 would be matched with a consistent enforcement of AML/CFT rules. This would close current loopholes and remove the weak links caused by insufficient cooperation and inconsistent approaches to supervision and to the risk assessment. Under option 3, the EU AML/CFT framework would be better able to effectively deal with cross-border cases and to significantly improve the detection of dirty money that has thrived on the current legislative fragmentation. The necessity of adopting a consistent approach to the AML/CFT framework that addresses all its parts in a holistic way has also been highlighted by stakeholders that took part in the public consultation on the present legislative proposals. Option 3 would also be the best option to address the need to reduce compliance costs to the minimum, especially for small and medium-sized market operators. From this viewpoint, the interaction with competent authorities is a substantial part of the AML/CFT related burdens, especially in cross-border business activities.

Both options 2 and 3 would include changes to substantive requirements in AMLD (more harmonised norms) and may hence entail compliance costs for private sector entities. However, for existing obliged entities these implementation and compliance costs would be *one-off and fairly limited*: adjustments would be required in internal processes and procedures, but are not expected to generate a need for significant investment in infrastructure or expensive technologies. Additional requirements on CDD, reporting etc. are not expected to require recruitment of extra staff or purchase of extra IT applications, and are broadly supported by stakeholders (see Annex 2). Once compliance with amended rules is ensured, no additional costs would be generated in comparison with on-going compliance costs under current rules (baseline scenario).[55]

For those entities which will fall under the scope of the EU AML rules for the first time, there will however be significant administrative costs; this mainly concerns certain Crypto Asset Service Providers (CASPs) but also crowdfunding service providers (discussed in Annex 6). The implementation of new rules on crypto assets will modify the conditions in which CASPs will exercise their activities. Thus, although wallet providers or exchange platforms between fiat and crypto currencies were already made obliged entities by the 5th AMLD, other type of services were not yet submitted to Customer Due Diligence and other reporting obligations, which will henceforth have to

[55] Existing compliance costs for OEs vary greatly, depending on the category of OE and size; one estimate is that for a medium-sized cross-border bank in the EU, the annual AML compliance cost is in the range US$41-54 million (LexisNexis: The True Cost of Financial Crime Compliance Report, March 2020).

be applied and which will generate new compliance costs (recruitment of relevant AML personnel, obtaining suitable IT tools and so forth).

In addition, the current proposal will introduce new specific requirements for both the newly-covered CASPs and those already covered in AMLD, in particular the so called "travel rule" requiring to obtain, hold and share required and accurate information on crypto asset transfers users and make it available on request to appropriate authorities[56]. These specific obligations raise various technical challenges, as crypto assets services providers have to develop technological solutions and protocols allowing to collect and share this information, both between themselves and with the competent authorities. Some European Union CASP representatives[57] claim that the absence of a standardised global, open source and free, technical solution for the travel rule could lead to the exclusion of small actors from the crypto-assets market, with only important players being able to afford compliance with the rules. However, no precise estimated costs were provided, and it must be noted that this requirement is an implementation of new global FATF standards which should be implemented around the world.

On the other hand, for obliged entities that are operating on a cross-border basis and are currently subject to divergent jurisdictional rules, significant compliance costs are generated by these differences, hence in the medium term harmonised rules would lead to cost-saving in compliance area, and for newly-covered entities, the additional costs would be mitigated. Furthermore, as noted in annex VI and section 8 below, one current category of Obliged Entity, traders in goods, will be removed from the scope of the AML/CFT framework in light of the envisaged ceiling on large cash transactions (see annex IX), and therefore save on compliance costs. This will also lead to savings for FIUs, which will no longer have to process notifications of such large cash transactions.

As regards international competitiveness of EU entities, in particular banks, while the EU regime already imposes a strict set of obligations, in many ways stricter that in other jurisdictions, the single rulebook is not likely to have any negative impact on competitiveness. On the contrary, the evidence from past alleged money laundering cases indicates that the reputational risks have a significant impact on the competitiveness of involved banks, which can be reduced by a stronger preventive framework.

Option 3 would additionally to option 2 entail administrative costs for Member States' supervisory authorities and FIUs that in some cases would need to adjust their powers and tools, with potential commensurate adjustment in human and financial resources. The adjustment would also be one-off and would swiftly bring benefits in terms of enhanced capacity and more efficient execution of their tasks.

[56] This "travel rule" requirement will be implemented via an amendment to Regulation 2015/847 on information accompanying transfers of funds. See Annex 6, section 8. It arises from FATF Recommendation 15 (with interpretative note).
[57] The Blockchain and Virtual Currencies Working Group notably raised this issue.

This option is supported by the public, which supported greater harmonisation in each of the areas presented for consultation. It is important to note that opposition to greater harmonisation was limited to at most one quarter of respondents, signaling a huge level of support for more harmonisation and consistency across the Union.

In conclusion, for the above reasons, the preferred option would be option 3.

	EFFECTIVENESS	*EFFICIENCY (cost-effectiveness)*	*COHERENCE*	*OVERALL SCORE*
Option 1 *Baseline scenario*	0	0	0	0
Option 2 *Coherent approach for supervised entities alone*	+	+	+	+
Option 3 *Coherent approach for both supervised entities and competent authorities*	++	+	++	++

Magnitude of impact as compared with the baseline scenario (the baseline is indicated as 0): ++ strongly positive; + positive; – – strongly negative; – negative; ≈ marginal/neutral; ? uncertain; n.a. not applicable

6.2 Improve the effectiveness and consistency of anti-money laundering supervision

Under the baseline scenario (option 1), the effectiveness of cross-border cooperation and information exchange between national competent authorities and other relevant bodies tasked with responsibilities in the area of AML, while enabled and encouraged in Union law, would remain predicated upon the willingness and capacity of individual authorities. The main mechanisms enabling such cooperation would not be regulated at Union level and would comprise of ad-hoc contacts, formal or informal AML colleges established by competent authorities in home jurisdictions, formal or informal Memoranda of Understanding (MoUs) between public authorities in some or all EU jurisdictions. The existing MoUs cover certain aspects of supervision where information-exchange needs arise which require on-going information exchange but do not purport to provide or establish an institutional cooperation framework or legal obligations with regard to exchange of information and enhancing the effectiveness of supervision at EU level.

In cases where AML-related weaknesses or compliance deficiencies in obliged entities have cross-border character or implications, a fragmented institutional framework would not be conducive to coordinating supervisory actions and designing measures that would address such weaknesses holistically and effectively. At the same time, differences in supervisory approaches would remain an obstacle for private sector entities that operate across several EU Member States to design effective, consistent, and high-standard group-wide policies and procedures for effective compliance with AML/CFT requirements.

In the non-financial sector, the status quo would continue, in which the landscape of national authorities and bodies tasked with various supervisory tasks vis-à-vis different

industry sectors is extremely diverse. No overview of cross-border cooperation and information exchange mechanisms is available or known to exist.

Option 2, while enabling important progress in strengthening the EU AML supervisory framework, especially in the non-financial sector, would still not address a few of the most fundamental deficiencies that exist at present. The institutional framework of AML supervision in the EU would remain fragmented. In contrast to prudential supervision in the Eurozone, even significant and risky cross-border entities would be subject to fragmented supervision across Member States. In a best-case scenario, effective cooperation and information exchange channels would exist between individual supervisory authorities, enabling an enhanced approach to risks. However, in cases where national authorities are unable to ensure an adequate level of supervision of a particularly risky entity or address a particularly complex situation which may have implications for the Union as a whole, there would be no EU-level mechanism or authority to address the problems and take appropriate measures directly vis-à-vis a specific entity. In such cases, deficiencies at the national level would threaten the resilience of the Union AML/CFT framework, making the EU as strong as its weakest link in terms of supervision.

Through coordination and oversight, this option would improve the understanding of sectorial risks and the quality of supervisory action in the non-financial sector, whilst fully respecting Member States' decision to delegate supervision in this sector to self-regulatory bodies.

In terms of costs, this option would necessitate a moderate incremental increase in resources for strengthening indirect supervision of the financial sector and additional funding and resources dedicated to indirect supervision of the non-financial sector at EU level. Under the reform of the European Supervisory Authorities, additional resources have been provided to the European Banking Authority (EBA) for strengthening of its AMLD mandate in the financial sector. A comparable increase would be required for establishing indirect supervision of the non-financial sector.

Option 3, in addition to the advantages available under option 2, by allowing for direct supervision of certain financial sector entities, would enable a proportionate and targeted approach for addressing issues related to institutional fragmentation and mismatch between the cross-border nature of ML/TF risks and single jurisdiction-focused supervision. Successful establishment and functioning of the Single Supervisory Mechanism (SSM) in banking has demonstrated that direct supervision of selected entities at EU level, designed as a system where national competent authorities and the EU centre cooperate and carry out their tasks jointly, can be more effective and efficient than purely national-level supervision.

In the area of AML/CFT, the intensity of supervision needed depends on the AML risk profile of an entity. Large financial sector entities with a high residual risk profile, significant cross-border presence and complex activities could be more efficiently supervised directly at EU level, because a single authority would have a complete view of the risk profile and risk exposure of the entire group, as opposed to a fragmented

picture of the risks in separate jurisdictions. In addition, EU-level supervision would better mirror the requirements that are also imposed on a group-wide basis, such as a single policy and common procedures that entities should have in place for all their operations in the Union.

Given that under option 3 the transfer of direct supervision powers to EU level would only concern a relatively limited number of risky and mostly cross-border entities, while the vast majority of financial sector entities as well as non-financial sector entities would remain supervised at national level, this option would address the fundamental issues of the baseline scenario while ensuring integrated Union-level supervision for cases where it brings the largest added value. The ability of the EU supervisor to take over supervision of any financial entity if a procedure confirms inadequate supervisory action by the national supervisor, would be an added safeguard reducing the realisation of ML/FT risk in the Union.

This option is supported by stakeholders, with 66% of respondents to the public consultation favouring a new body over the EBA, and a majority of views advocating for a broad coverage of sectors, whether from the outset or in subsequent phases.

The option is also in line with principles of proportionality (involving sufficient but not excessive powers and resources allocated to EU level) and subsidiarity (considering that national supervisory authorities would not be substituted but would remain part of the integrated supervisory system even in cases where direct supervision is transferred to EU level and such direct EU supervision would only cover entities for which there is evidence that national action alone cannot suffice).

With regard to costs, in comparison with Option 2 which would present only an incremental increase in the already existing funding of Union level indirect supervision, this option would additionally require an establishment of direct supervision function at Union level, properly staffed and funded. The resources necessary for direct supervision could be financed mainly via levying of fees from directly or indirectly supervised entities. This would follow the practice of supervision financing in the majority of Member States and in the Single Supervisory Mechanism, where the ECB supervision is financed via fees from supervised entities. A preliminary estimate of resource needs of such an Authority would be approximately 250 full time staff with a budget of approximately EUR 40 million[58]. National supervisors currently supervising entities which pass to the EU Authority for direct supervision would experience some cost saving, but it is not anticipated that they will reduce staff but rather reallocate freed staff for more effective supervision of other entities remaining under national supervision.

In the short term, as evidenced by the SSM experience and that of ESMA (which supervises trade repositories and credit rating agencies), the fees levied from entities represent *additional* cost for the private sector, as they come on top of financing national level supervision. However, given that majority of entities selected for direct EU level

[58] More details in annex 5.

AML supervision would be large and cross-border, the benefit of efficiency effectiveness of the single EU level supervision based on harmonised standards would present the benefits outweighing these costs and acknowledged by respondents to the public consultation, including private sector entities, who view the potential establishment of EU supervision positively[59].

With option 4, the extent and complexity of the full-scale transfer of responsibilities and powers related to direct supervision from national level to the EU level would be unprecedented. To take the example of Sweden only, this would require the EU supervisor to take over the supervision of more than 20.000 entities. Even in the case that such option were to only include financial sector entities, the EU supervisor would have about 2.000 entities under its direct supervision. Such extent of exercise of supervisory powers is unprecedented. Even in the case of prudential banking supervision in the Eurozone, direct supervision tasks and powers are distributed among the EU-level (SSM) and national level (national competent authorities). This option would require a long multi-annual transitional period for accommodating the transfer and achieving a greater level of effectiveness and efficiency in supervision than currently available at national level. Considering that the supervision of the majority of entities subject to AML requirements is performed adequately at national level, and the risks most entities pose are related to the specific national context, the option may raise both proportionality and subsidiarity concerns.

This option would also present very significant costs in terms of financial and human resources that would be required for directly supervising all financial sector entities (numbering in the thousands). The resources located at EU level would need to approach the sum of resources currently deployed at national level. These additional costs that would have to be allocated to supervised entities would not be commensurate with the risk profile of individual entities, which could be low or moderate, and would not present the benefits of more efficient supervision for entities that can already be adequately supervised at national level.

The preferred option is therefore option 3, a combination of direct and indirect supervisory powers in an EU-level supervisory body in the form of a decentralised agency[60].

	EFFECTIVENESS	***EFFICIENCY (cost-effectiveness)***	***COHERENCE***	***OVERALL SCORE***
Option 1 *Baseline scenario*	0	0	0	0
Option 2 *Indirect supervisory powers*	+	+	++	+
Option 3 *Combination of direct and indirect supervisory powers*	++	+	++	++

[59] See annex 2 on the public consultation.
[60] The question of whether this agency should be an entirely new body or whether some or all of the new powers should be given to an existing agency, such as the EBA, is considered in annex 5.

Option 4 *Direct supervisory powers only*	+	--	++	≈

Magnitude of impact as compared with the baseline scenario (the baseline is indicated as 0): ++ strongly positive; + positive; – – strongly negative; – negative; ≈ marginal/neutral; ? uncertain; n.a. not applicable

6.3 Increase the level of cooperation and exchange of information among Financial Intelligence Units

Under the baseline scenario, the EU FIUs' Platform would continue to operate as an informal expert group, without any funding for dedicated training programmes, nor means to host the FIU.net system, nor build capacity in national FIUs, including through IT tools. This scenario does not provide the EU FIUs' Platform with any legal basis to issue binding standards, templates and guidelines in the area of work of FIUs (for example, formatting of STRs).

This would mean that the EU FIUs' Platform would be equipped with neither enhanced operational capabilities, nor legal means to coordinate and harmonise practices and templates among FIUs, to support the detection of suspicious cross-border transactions and to boost capacity of national FIUs. The absence of a stable and dedicated hosting for FIU.net[61] would compromise FIUs' ability to exchange information and to match data to detect information of interest for their financial intelligence analysis.

Under option 2, none of the weaknesses listed under option 1 relating to the operational aspects would be remedied. However, there would at least be a mechanism for the harmonisation of templates and standards, which would facilitate cooperation among FIUs. Yet, under this option the Commission would have full control over the process for adopting such templates and standards and their content, which runs contrary to the principle of operational independence and autonomy enshrined in the AML Directive and upheld by FATF standards.

Option 3, in addition to option 2, would allow reinforced operational capabilities and support joint analyses by drawing up common procedures and providing the necessary technical and administrative support to national FIUs. A strong support and coordination mechanism would facilitate and speed up the detection of suspicious cross-border transactions and activities, enabling to disseminate quickly and effectively relevant information among national FIUs. FIUs would have common templates and methodologies for cooperation and would maintain their operational autonomy due to having developed and adopted those common templates and methodologies themselves in full independence. Cooperation between FIUs is likely to be significantly enhanced. Better feedback from FIUs to obliged entities would be promoted, leading to a reduction

[61] See footnote 48 above. Commission hosting of FIU.net is seen as a temporary solution (Action Plan, p11): "*In the short term, the Commission will take over the management of the FIU.net in order to ensure the continuous and uninterrupted functioning of the system. In the longer term, the EU coordination and support mechanism could be tasked with hosting the FIU.net or its successor. Other suitable solutions could be considered*.".

in over-prudent submission of excessive numbers of STRs, and reducing the false positives discussed above in section 2.1.

This option is supported by the public, with respondents across all stakeholder groups favouring a broad array of tasks for the FIU support and coordination mechanism. While views on the hosting of the mechanism were more split, the future AML/CFT supervisor was the option receiving the broadest support.

As regards Option 4, concerning the legal basis, replacing all national FIUs with a single EU FIU, while potentially addressing all the issues stemming from the current decentralised setup and necessity of cooperation between national FIUs, requires very far-reaching legislative actions and reforms in areas going beyond the legal basis for the current proposal.

Secondly at operational level and by the very nature of their competences, besides financial expertise, FIUs operate as intelligence services and their efficiency is based on their access to a series of other sources of information at national level. In order to carry out its core task of analysis of received STRs, the EU FIU would depend to a very large extent on data available at national level, and thus require access to and ability to process all such data and information currently available exclusively to national FIUs, including for example police, judiciary, customs, taxation information and databases. In the absence of such access, the intelligence produced by such an EU FIU would be of poor quality and of little to no use to law enforcement and other competent authorities. Furthermore, an EU FIU could trigger, where appropriate, a question on the competence to undertake criminal investigation currently organised at national level.

Thirdly, the EU FIU would need to have an operational capacity to carry out the tasks of all national FIUs, amounting to the need of human and budgetary resources equalling at least the sum of all resources currently allocated at national level. The cost of closing down national FIUs and transferring all functions to an EU FIU would be significant, and interruption of service would be a serious risk.

Lastly, there is currently a strong opposition from Member States to a centralised EU FIU of any form[62].

Option 3 (an FIU support and coordination mechanism as part of an EU AML Authority) is therefore the preferred option.

	EFFECTIVENESS	***EFFICIENCY (cost-effectiveness)***	***COHERENCE***	***OVERALL SCORE***
Option 1 *Baseline scenario*	0	0	0	0

[62] See Council conclusions on enhancing financial investigations to fight serious and organised crime, 8927/20 17 June 2020 recalling that it is the prerogative of the Member States to choose a model for their FIU which best fits their legal and administrative system" (p.10), EU/EEA Financial Intelligent Units Joint position paper, 09/02/2020.

Option 2 *Commission delegated/implementing regulatory power*	+	++	+	+
Option 3 *FIU support and coordination mechanism as part of an EU AML Authority*	++	+	++	++
Option 4 *Single EU FIU*	-	--	++	-

Magnitude of impact as compared with the baseline scenario (the baseline is indicated as 0): ++ strongly positive; + positive; – – strongly negative; – negative; ≈ marginal/neutral; ? uncertain; n.a. not applicable

7 PREFERRED OPTIONS

7.1 Effectiveness

Increased effectiveness of enforcement of AML/CFT rules is the principal objective of the present initiative. This should reduce the quantity of funds which are laundered or used to finance terrorism, either through greater detection or deterrence to criminals, with significant social benefits. The proposed new EU AML supervisor is at the heart of this envisaged increased effectiveness, both through its role in directly supervising a number of the most risky entities, and its indirect supervision and coordination of national AML supervisors. Greater cooperation between FIUs should also increase their effectiveness in quickly identifying, from the many STRs which are submitted to them, those which are genuinely likely to be connected to cross-border ML/FT activities and act quickly to stop those transactions and inform law enforcement authorities. Directly applicable rules in a single rulebook contribute to effectiveness by reducing the time taken by national transposition and the small divergences of detail which can arise during the transposition process.

7.2 Efficiency

Under this heading, on the negative side, it must be considered that there are significant financial costs associated with the preferred options, in particular the option to create an EU level supervisor with some direct supervision functions, integrating the FIU platform within this supervisor, and for entities newly covered by the scope of AML legislation. Regarding the supervisor, while the main part of its budgetary costs can be raised by fees levied from financial sector entities across the EU, this will represent a burden to them (of a total amount of approximately EUR 30 million, see Annex 5).

Furthermore, the role of a new EU AML Authority will enhance the efficiency of operations of EU AML supervisors via increased coordination and dissemination of best practices. Direct supervision of selected cross-border entities would also be both more effective and efficient than the current fragmented approach, where a single obliged entity faces a multiplicity of supervisory authorities and approaches. The additional power to take over supervision of certain entities from national supervisors in defined

cases of inaction or unsuitable practices by the national supervisors will act as a motivating factor on them to supervise efficiently. Harmonisation of formats and templates used by FIUs will render cooperation between them more efficient, as will a central coordination role of a formalised EU FIUs' platform. Overall, it is anticipated that the efficiency of enforcement of AML/CFT rules will be enhanced in the EU as a whole by the new organisational setup.

The additional costs for CASPs (discussed above in 6.1.), reflect the fact that crypto assets are identified as a risk area for ML/TF, and will bring them into line with other entities engaged in the transfer of funds and assets. The benefits of reduced ML and TF activity mainly accrue to society as a whole, not directly to Obliged Entities, and it is therefore on the level of overall social welfare that efficiency should be considered; OEs are in a sense performing a service to society by monitoring possible criminal activity. However, better internal AML/CFT practices within financial institutions and other OEs can enable them to avoid sanctions for breaches of AML/CFT rules, with the prospect of a direct benefit, and also bring reputational benefits (indeed, the very fact of being included within EU AML/CFT legislation could bring such CASPs greater confidence from consumers).

7.3 Coherence

7.3.1 General remarks on coherence

In addition to the benefits of the preferred options in each of the areas (harmonised rules, EU supervisor and EU FIUs' Platform), as described in section 6 above, the coherence of the preferred options with each other, and their benefits considered as a package should be considered. A harmonised rulebook is a prerequisite for direct supervision of certain entities at EU level and will considerably facilitate the task of indirect supervision and coordination of national supervisors by an EU supervisor. The EU supervisor, when operating at full capacity, will have a range of tasks in the areas of supervision regulation and coordination, allowing a more joined up approach to AML/CFT enforcement across the EU; it will be regarded as the centrepiece of the proposed reforms. FIUs are key components of this enforcement, and so far have needed to rely on suboptimal coordination mechanisms and unharmonised communication formats. Through participation in an EU Authority, the FIU community would be closely associated to policy dialogue, by analysing money laundering methods and risk typologies, drawing large scale trends and European threats, suggesting priorities, and discussing policy proposals and initiatives[63]. The interaction would therefore benefit both supervision as well as strategic analysis of the FIUs. It is estimated that the three preferred options when applied together will interact with each other positively in such as a way as to magnify the benefits of each option individually.

[63] It is not feasible nor cost-effective to create a new EU Agency only for the central body of FIUs, if it were not decided to create an EU Agency/Authority for AML more generally; without such an Agency, option 2 would have to be retained as regards the strategic objective of enhancing cooperation among FIUs.

7.3.2 Coherence between the preferred options and other Commission policies

EU action to prevent money laundering and terrorist financing covers a vast number of sectors. As such, it interacts with several EU sectorial policies. The Action Plan of 7 May had identified inconsistency in how these sectorial and AML/CFT rules interact. While not all instances of inconsistency can be addressed by a more harmonised set of AML/CFT rules, the preferred option will increase policy coherence as follows:

- More harmonised rules on customer due diligence, clearer identification of the objectives of CDD and of the use that can be made of the information obtained for this purpose will reduce the discretion left to credit institutions as regards when they should refrain from entering in a business relationship or terminate an existing one. Coupled with the upcoming review of the Payment Account Directive, this will reduce the impact on legitimate transactions and ensure improved access to basic financial products, hence increased financial inclusion, whilst allowing adequate mitigation of money laundering and terrorist financing risks.
- Clearer customer due diligence rules will also streamline the application of AML/CFT checks in the context of pay-outs when banks are wound up or declared insolvent.
- Time limits for FIUs to suspend transactions will reduce the exposure of credit and financial institutions to litigations by their clients, thus reducing the tension between their commercial and AML/CFT duties.
- The explicit authorisation to resort to remote identification and verification of customer identities is consistent with Commission plans to review the e-ID regulation.
- Consolidating the list of Obliged Entities under AML/CFT rules will be conducive to a better focus on those categories of service providers that can act as gatekeepers of our financial system, whilst avoiding that those service providers that have no exposure to money laundering / terrorist financing risks are unduly subject to AML/CFT requirements.
- The inclusion of crypto asset service providers among the entities subject to AML/CFT rules and the introduction of a traceability requirement for transfers of crypto assets will complement the recent Digital Finance Package of 24 September and will ensure full consistency between the EU framework and FATF standards.
- The approach taken to identifying entities subject to AML/CFT rules will also ensure consistency with the recently adopted European crowdfunding service providers Regulation[64], in that it provides the evidence in support of subjecting crowdfunding platforms to AML/CFT rules.

[64] Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business. OJ L 347/1 of 20.10.2020.

Further, the preferred option will provide more clarity on the interaction between competent authorities and with other authorities such as law enforcement and customs and tax authorities. This will close the current gap in relation to exchange of information between customs and FIU in relation to cash declarations by ensuring that FIUs provide sufficient feedback to customs in relation to such cash movements.

The preferred option will maintain the current coherency the existing policies under the criminal law framework, in terms of criminalisation of money laundering (Directive 2018/1673[65]) and terrorist financing (Directive 2017/541[66]). The proposed interconnection of the central bank account registries is also coherent with Directive 2019/1153 on the use of financial information to combat serious crimes[67], as it does not preclude nor prejudge Member States transposition, due by 1 August 2021, whilst allowing further access to the interconnection by law enforcement authorities once the scope of such access has been defined at national level. Finally, the preferred option is coherent with the provisions of Directive 2014/42/EU[68] which establishes a common set of minimum rules on the freezing and confiscation of instrumentalities and proceeds of crime and aims to prevent criminals from expanding their illicit activities and infiltrating the legal economy, as it will increase the level of defence of our financial system against criminals.

The European Commission adopted on 24 September 2020 a digital finance package, including a digital finance strategy and two legislative proposals, one on crypto-assets and the other on digital resilience[69]. The strategy sets out priorities such as removing fragmentation in the Digital Single Market, adapting the EU regulatory framework to facilitate digital innovation and addressing the challenges and risks with digital transformation that should also contribute to the objective of combating money laundering and the financing of terrorism.

[65] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284, 12.11.2018, p. 22–30.
[66] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, p. 6–21.
[67] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, OJ L 186, 11.7.2019, p. 122–137
[68] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union, OJ L 127, 29.4.2014, p. 39–50
[69] See https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

The draft regulation on crypto-assets provides a legal framework for crypto-assets and crypto assets services providers, including a definition of 'crypto-assets' and a list of recognised crypto-asset services that transposes in the EU law the recommendations of the Financial Action Task Force. Other provisions of the draft regulation on licensing and registration requirements, rules for supervision, preservation of financial stability and investors protection will be cross-referred in this legislative proposal.

7.3.3 Coherence between the preferred options and the EU data protection framework

The preferred options intersect in several areas with the fundamental right to personal data protection, which is enshrined both in the EU Charter of Fundamental Rights (Article 8) and in the Treaty on the functioning of the European Union (Article 16). The fundamental right to the protection of personal data is not an absolute right, however limitations to this right must be strictly necessary according to settled CJEU case-law. Nevertheless, the objective of fighting money laundering and terrorism financing, which endanger both the financial system and the security of citizens of the European Union must be properly balanced, in the light of, against this right subject to the the principles of necessity and proportionality.

The current European AML/CFT legislation already takes this necessary balance into consideration, notably in Chapter V of the AML Directive, on "Data protection, record-retention and statistical data", which contains explicit references to the EU data protection framework[70] and where the processing of personal data on the basis of the AML Directive for the purposes of the prevention of ML/TF is already explicitly recognized as a matter of public interest under Regulation 2016/679 (GDPR)[71].

In any case, legislative proposals must be fully consistent with the European data protection framework. The EDPS will be consulted on the package of legislative proposals accompanied by this Impact Assessment, in accordance with Article 42 of Regulation 2018/1725, to ensure that all data protection requirements are duly taken into account.

The EDPS adopted an Opinion in July 2020 on the Commission's action plan acknowledging the importance of the fight against money laundering and terrorism financing as an objective of general interest [72]. The EDPS welcomed areas where the

[70] Article 41.1 "The processing of personal data under this Directive is subject to Directive 95/46/EC, as transposed into national law. Personal data that is processed pursuant to this Directive by the Commission or by the ESAs is subject to Regulation (EC) No 45/2001". As both Directive 94/46/EC and Regulation (EC) 45/2001 have been replaced, respectively, by Regulation (EU) 2016/679 and Regulation (EU) 2018/1725, these references should be updated in the new legislative proposal.

[71] Article 43 "The processing of personal data on the basis of this Directive for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 shall be considered to be a matter of public interest under Regulation (EU) 2016/679 of the European Parliament and of the Council."

[72] EDPS Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, available at https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf

Action Plan focusses on convergence with data protection rules, but also highlighted areas where impacts on the rights to privacy and to personal data protection will have to be carefully considered.

Regarding areas of convergence, the EDPS welcomed the envisaged harmonisation of the AML/CFT framework through the adoption of a Regulation, i.e. the preferred option retained for objective 1, as this will result in a direct and more consistent application of the main rules by Member States as well as a uniform interpretation by the Court of Justice of the European Union.

The set-up of an EU-level supervisor did not raise specific issues by the EDPS, Regarding the suggestion to have a specific legal basis for it to process personal data as well as the necessary data protection safeguards, particularly regarding information sharing and international transfers of data, this will be duly taken into account when drafting the corresponding legislative proposals.

Regarding Financial Intelligence Units, the preferred option of establishing the mechanism for the support and coordination of FIUs clarifies the conditions for access to and sharing of information on financial transactions by FIUs, as requested by the EDPS. In particular, the preferred option does not review the handling of personal data for the purpose of producing financial intelligence, which remains solely the task of national FIUs as it is currently the case. The support and coordination mechanism will only centrally coordinate at strategic level, without having any access to the content of suspicious activity or person. The preferred option provides also a suitable solution for the management of FIU.net that is in line with the GDPR and the data protection framework, as it will ensure that full control over the management and processing of personal data is entrusted to the FIUs. This element is essential, as the EDPS underlined.

The EDPS Opinion welcomed the use of public-private partnerships (PPPs) for the exchange of information on typologies and trends by FIUs and law enforcement to obliged entities. On the other hand, the EDPS expressed concerns that the use of PPPs for the sharing of operational information on intelligence suspects by law enforcement authorities to obliged entities would lead to a high risk for the individuals' rights to privacy and data protection. For this reason, the Commission, as indicated in the Action Plan, envisages to request the European Data Protection Board (EDPB) for Guidance in this area.

The areas concerned by enhanced harmonisation (such as the list of obliged entities, customer due diligence requirements, internal controls, reporting obligations, provisions on beneficial ownership registers and central bank account mechanisms), involve the processing of a substantial amount of personal data. Therefore, the EDPS Opinion underlined that possible concerns about data protection require careful attention in order to be mitigated, notably as regards the following aspects:

- Compliance by FIUs when engaged in enhanced coordination and data exchange with data protection rules will include conditions of access and sharing

information, including on international transfers of personal data. Moreover, the conditions for sharing information between these authorities should include appropriate technical and organisational measures, to protect data against accidental or unlawful destruction, accidental loss, alteration or unlawful disclosure, including encryption and anonymization. This will be ensured by allocating stable and dedicated resources to the FIU support and coordination mechanism, which will ensure that the channels and methods for data sharing are fully in line with data protection rules.

- Digitalised CDD must be accompanied by the necessary measures to ensure the security of personal data, and in particular measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage (integrity and confidentiality). Moreover, the digitalisation of CDD processes should be driven by the data protection-by-design principle. This will be ensured through the adoption of Regulatory Technical Standards (RTS) in full compliance with the requirements of the AML Directive that any secure, remote or electronic identification process needs to be regulated, recognised and accepted by the relevant national authorities (Article 27), and in full compliance with data protection requirements.

  More generally, the use of technological solutions (such as artificial intelligence or databases used by obliged entities to access information relevant for carrying out customer due diligence), which might help to improve detection of suspicious transactions and activities, must be in line not only with international and EU AML/CFT standards but also conform to other EU rules, including on data protection and antitrust. The Commission will consider requesting formally the EDPB to produce specific Guidance with regard to data protection requirements in these areas.

7.4 Summary of impacts of selected options

Objectives / *Policy option*	*EFFECTIVENESS*	*EFFICIENCY (cost-effectiveness)*	*COHERENCE*	*OVERALL SCORE*
1. Baseline scenario	*0*	*0*	*0*	*0*

Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards				
Option 3 *Coherent approach for both supervised entities and competent authorities*	++	+	++	++
Improve the effectiveness and consistency of anti-money laundering supervision				
Option 3 *Combination of direct and indirect supervisory powers*	++	+	++	++
Increase the level of cooperation and exchange of information among Financial Intelligence Units and when appropriate with other competent authorities				
Option 3 *FIU support and coordination mechanism as part of an EU AML Authority*	++	+	++	++

8 REFIT (SIMPLIFICATION AND IMPROVED EFFICIENCY)

No evaluation of the existing AML Directive has taken place to date prior to the preparation of the present impact assessment (see annex 4). The transposition deadline of the fourth AMLD was June 2017, and the transposition deadline of the fifth AMLD was January 2020. In both cases a number of Member States did not transpose on time and infringement proceedings were launched. The assessment of completeness and conformity of transposition by the Commission is still ongoing for both Directives. Article 65 of the consolidated AML Directive requires the Commission, by 11 January 2022 and every three years thereafter, to submit a report on the implementation of the Directive in the Member States. However, given transposition delays, there is not yet a series of three years of data on implementation of the fourth AMLD, much less the fifth.

The reasons behind the urgency of the AML Action Plan of May 2020, and of the legislative package accompanied by this impact assessment, before evaluation of the existing AML Directive, are explained in the Introduction and in Annex IV. The primary objective of the present proposals is to increase the effectiveness of the EU AML/CFT regime, with the aim of reducing the amount of criminal ML/FT in the European Union, rather than simplification and improved efficiency.

Nevertheless, a number of elements of the proposed measures will further simplification and improved efficiency, even though the present initiative does not repeal any EU legislation:

- The replacement of certain rules in a Directive with more harmonised and directly applicable rules in a Regulation, will remove the need for transposition work in the Member States and facilitate doing business for cross-border entities in the EU.

- Those large and cross-border financial entities which will be directly supervised by the EU AML Authority will no longer have to deal with multiple AML supervisors in different Member States, which will simplify AML supervision for them.

- The removal from the scope of the EU AML framework of traders in goods, referred to in Annex VI and linked to the proposed prohibition on cash operations over EUR 10 000 described in Annex IX, will release such traders from the administrative burden of submitting to their FIU reports on cash operations exceeding EUR 10 000.

- The greater degree of harmonisation of AML rules in a number of specific areas will simplify cooperation between supervisors and FIUs due to the reduction in divergences between their rules and practices.

- The creation of an FIU coordination mechanism will simplify and facilitate cooperation between FIUs.

9 HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

An evaluation of the present package will be carried out in principle five years after its entry into application. While it is by definition impossible to know how much undetected criminal activity in the area of ML/TF is taking place, it is possible to measure outputs in terms of the effectiveness of the EU AML/CFT framework that will ensue from the combination of the above preferred options. The monitoring tools proposed below go beyond the pure compliance with the framework and follow international best practices set out by the Financial Action Task Force to assess the effectiveness of jurisdictions in preventing and fighting money laundering and terrorism financing.

The main impact of the enhanced rulebook will be an improved application and enforcement of the rules.

At the level of the obliged entities, this can be measured in several ways.

The number of STRs generated is an intermediate indicator, and not totally reliable, as an obliged Entity can theoretically generate many thousands of STRs, overwhelming its FIU. Better performance of obliged Entities in generating only useful targeted STRs should be aimed at, and can be evaluated on the basis of feedback from FIUs.

The non-financial sector so far generates relatively few STRs, therefore an increase in the volume of STRs generated by that sector should be aimed at.

A more effective indicator would be the quality of the STRs themselves, which could be measured as a ratio of the STRs deemed useful for the production of financial intelligence out of all the STRs received by FIUs.

Another indicator could be the evolution in supervisory measures taken vis-à-vis obliged entities. This is expected to intensify horizontally in a first phase, whereas it should become more stable in the medium to long term as those entities improve their AML/CFT systems.

In relation to supervision, several indicators can be used to monitor the impact of the measures proposed.

The number of EU-wide methodologies developed for the identification and assessment of horizontal and sectorial risks is expected to increase, compared to the current absence of such common tools at EU level.

Based on common methodologies, it is expected that also those supervisors that have less means will be in a position to produce sectorial risk assessments. This indicator is therefore expected to grow.

As an effect of the oversight role of the EU supervisor, it is expected that the intensity of supervision will grow for each sector.

Similarly, based on the products produced at EU level, it is expected that guidance to obliged entities will both increase and become more frequent.

As regards the FIU support and coordination mechanism, one key indicator to monitor and evaluate the impacts of the measure concerns the usefulness of FIU disseminations of analyses to law enforcement authorities and other competent authorities. As a result of the support provided by the mechanism, it is expected that the number of investigations started on the basis of financial intelligence provided by the FIU, or supported by it, will increase.

More effective activity of FIUs in treating the STRs which they receive should contribute to this.

The volume of information exchanged among FIUs is one indicator of improved cooperation, and can be generated by FIU.net.

Additional indicators to monitor the impact of the measures proposed will be the share of STRs analysed, which is expected to grow in line with better tools available to FIUs, as well as an increase in the production of strategic trends and analyses of money laundering and terrorist financing methods.

An increase in the feedback provided to entities subject to AML/CFT rules is also expected, which will in turn contribute to the quality of the STRs submitted by those entities.

Summary of indicators:

Objectives	Indicator	Source of information
Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards	Numbers of STRs transmitted to law enforcement authorities	FIUs
Improve the effectiveness and consistency of anti-money laundering supervision	STRs generated by non-financial sector Proportion of all STRs which can be used for financial intelligence	FIUs
Increase the level of cooperation and exchange of information among Financial Intelligence Units	Volume and nature of information exchanged among FIUs increase in feedback to obliged entities	FIU.net FIUs

ANNEX 1: PROCEDURAL INFORMATION

1. Lead DG, decide planning/CWP references

This Impact Assessment Report was prepared by Directorate D "Bank and financial institutions" of the Directorate General "Directorate-General for Financial Stability, Financial Services and Capital Markets Union" (DG FISMA).

The Decide Planning references are:

- PLAN/2020/7886: Revision of EU rules on Anti-Money Laundering (recast). Amendment of Directive of the European Parliament and the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing (recast of Directive (EU) No 2015/849).
- PLAN/2020/7907: Revision of EU rules on Anti-Money Laundering (new instrument). Proposal for a Regulation of the European Parliament and the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing, amending Directive (EU) No 2015/849.
- PLAN/2020/7908: EU Anti-money laundering supervisor. Proposal for a Regulation of the European Parliament and the Council on the establishment of a Union anti-money laundering supervisor.
- PLAN/2020/7909: EU rules on Anti-Money Laundering – establishment of a support coordination mechanism for Financial Intelligence Units. Proposal for a Regulation of the European Parliament and of the Council on establishing a coordination and support mechanism for Financial Intelligence Units.

The initiative on implementing the Commission Action Plan on Anti-Money Laundering and Countering the Financing of Terrorism was included in the 2021 Commission Work Programme published on 19 October 2020.

2. Organisation and timing

Three Inter-Service Steering Group (ISSG) meetings were held in 2020. The ISSG consisted of representatives from various Directorates-General of the Commission: HOME, ECFIN, BUDG, OLAF, REFORM, JUST, DIGIT, CLIMA, and SJ. The ISSG met on 15 July 2020, 1 October 2020 and 28 October 2020. The meetings were chaired by SG.

The contributions of the members of the Steering Group have been taken into account in the content and shape of this impact assessment.

3. Consultation of the RSB

The Impact Assessment report was examined by the Regulatory Scrutiny Board (RSB) on 2 December 2020. The RSB gave a positive opinion on 4 December 2020.

4. Evidence, sources and quality

A number of inputs and sources of data were used in the preparation of this impact assessment, including the following:

- Advice from the European Banking Authority, delivered to the Commission on 10 September 2020, and other reports of the EBA and other ESAs referred to in footnotes to this impact assessment.
- Evidence supplied in the context of the public consultation described in Annex 2.
- Data supplied by Member States in response to the sending of a questionnaire by the Commission on 31 July 2020, with responses provided during September 2020, covering in particular the activities of Financial Intelligence Units.
- Publications of the Platform of EU FIUs, referred to in footnotes to this impact assessment.
- Various reports from Europol, referred to in footnotes to this impact assessment.
- Various reports of the FATF, including Mutual Evaluation Reports of certain EU member States.

The data sources are thus essentially public authorities in the EU and its Member States. The quality of this data is therefore high, with the proviso that it covers essentially the activity of public bodies in the area of supervision enforcement and investigation in the AML/CFT field, and cannot reveal the amount of undetected money laundering and financing of terrorism.

Regarding alleged criminal ML/TF activity, outside of proven cases following full investigation, some indicative evidence comes from investigative journalism, some of it based on unlawfully obtained information. Such sources are by their nature partial and uncertain.

ANNEX 2: STAKEHOLDER CONSULTATION

1. Introduction

One of the Commission's priorities is to deliver an economy that works for people. As part of this overarching priority, the Commission set out to put forward a new, comprehensive approach to fighting money laundering and the financing of terrorist activities.

The Commission established this goal from the beginning of its mandate, building on the findings of the 2019 Anti-Money Laundering Package. This approach has the political support of both the European Parliament and the Council, as well as from the large parts of the private sector, which recognises that the EU cannot tolerate another wave of cases.

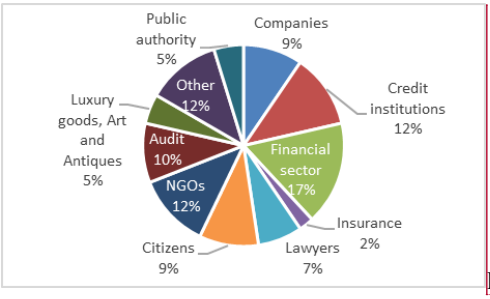
The results of the consultation activities presented in this Annex must be read in this context, bearing in mind that extensive exchanges of views have taken place since 2018, thus before the announcement and adoption of the Action Plan of 7 May, which this annex covers, and continue today.

2. Consultation strategy

In order to ensure that the Commission's proposal adequately takes into account the views of all interested stakeholders, the consultation strategy supporting this initiative has been built on the following components:

- A consultation on the roadmap announcing the Commission's Action Plan;
- A public consultation on the actions put forward in the Action Plan, open to the general public and all stakeholder groups;
- A targeted consultation of Member States and competent AML/CFT authorities;
- A request for advice from the European Banking Authority;
- An opinion of the European Data Protection Supervisor, and
- A final high-level conference bringing together representatives from Member States, competent authorities, academia, civil society and the private sector.

The results of each component are presented below.



3. Feedback on the roadmap

Commented [TJ1]: This shape has been converted to an inline shape. Please check the position.

A roadmap announcing the AML/CFT Action Plan of 7 May was announced on the Commission's "Have Your Say!" Portal. The consultation period ran between 11 February and 12 March 2020, and received 42 contributions from a varied range of stakeholders (see graph).

Most feedback supports increasing the level of effectiveness of the EU AML/CFT framework through more harmonised rules, including for crypto assets, which should both allow to treat different risk situations in different manners and remove current inconsistencies with other pieces of legislation (e.g. payment account directive), which make it difficult for some groups to achieve financial inclusion.

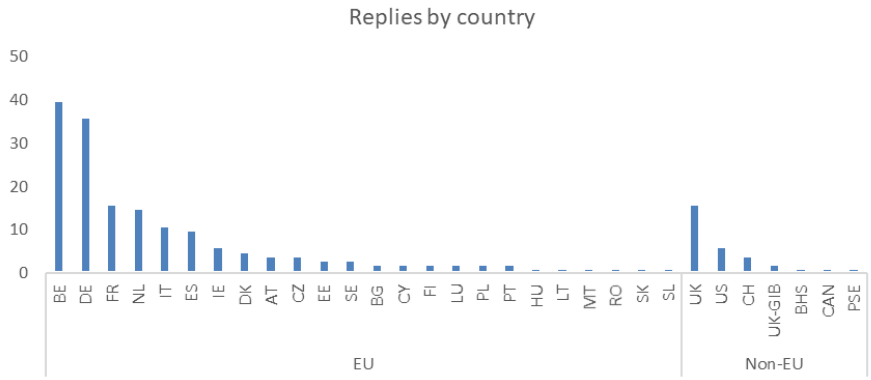
As regards authorities, the feedback calls for providing more tools to FIUs and for setting up an EU-level supervisor. Many respondents also asked for improved exchange of information, including through public-private partnerships. Contrary to the majority opinion, some representatives from the non-financial sector considered the current functioning of the framework satisfactory.

Finally, a roadmap on the access of law enforcement authorities to the interconnection of national centralised bank account registers and data retrieval systems was published on the Commission's "Have Your Say!" Portal. The consultation period ran between 31 March and 28 April 2021 and received 4 contributions from citizens and a business association, recognizing the importance for law enforcement to have swift access to bank account information in a cross-border context as well as the need for robust safeguards to ensure proportionality and respect for fundamental rights.[73]

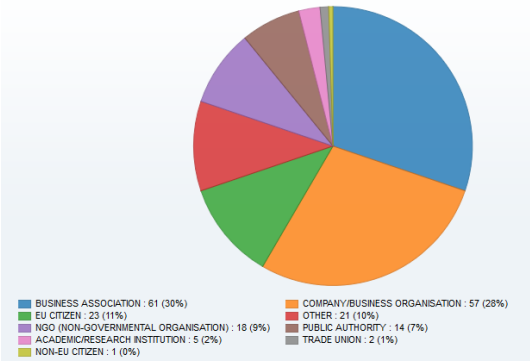
4. Public consultation

The public consultation was launched on 7 May, in parallel to the adoption of the AML Action Plan, and ran until 26 August. The consultation received 202 official contributions, while 7 additional replies were submitted informally. Replies were received from 24 of the 27 EU Member States, and from 6 non-EU countries.

[73] For more information: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12935-Cross-border-investigations-law-enforcement-access-to-interconnected-bank-account-registries_en.



The majority of respondents are private sector representatives (58%), with EU citizens, NGOs and academia accounting for 22% of replies. 7% of respondents are public authorities.



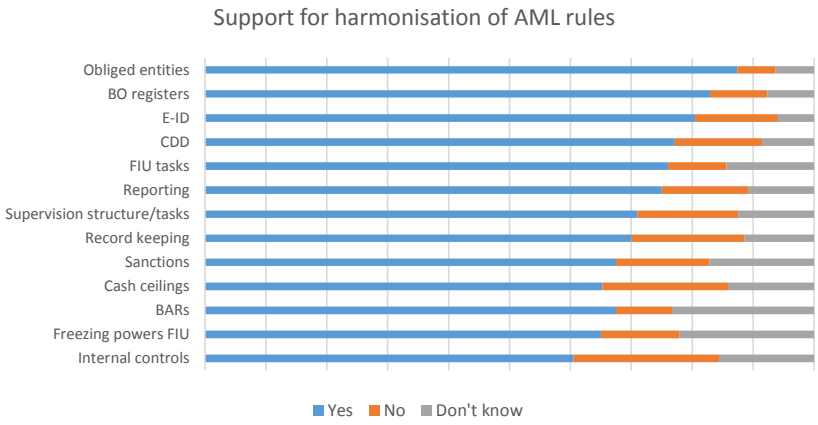
Below is a summary of the views expressed with regard to future EU action in the AML/CFT field, including in relation to the 3 pillars of the Action Plan that are covered by this impact assessment.

Need for action

Respondents widely believe that further action is needed to combat money laundering and terrorism financing (only 1% consider current action sufficient). In recognising the cross-border nature of such crimes, respondents consider that action at national level alone will not be effective. There is a widespread perception that effective results can be achieved at national level with support from the EU (39% vs 16%), and even more at EU level (54% vs 8%). Further, it is recognised that AML/CFT can only be tackled effectively through international cooperation (46% vs 6%). The need for action at supra-national level is perceived by all stakeholder groups. However, the appreciation of the effectiveness of national action varies, with public authorities being more prone to consider that national action can be effective than operators in the private sector. Citizens also consider action at EU level the most likely to yield positive results.

Pillar 2 – Harmonisation of the rulebook

As the graph below shows, the public consultation confirmed support from the public for harmonisation of all the rules put forward by the Commission for consultation, with little to no variation in the support across stakeholder groups. Yet, in the private sector views are more split between operators in the financial sector, who demand further harmonisation, and operators in the non-financial sector, who are opposed to more harmonised rules.



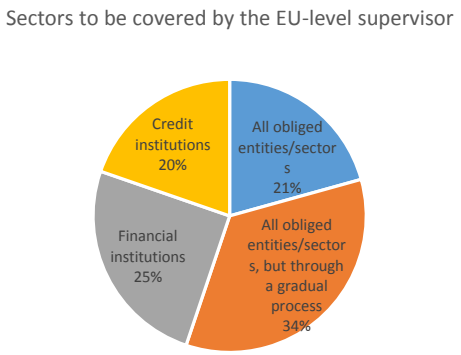
Beyond the areas presented in the graph above, the private sector indicated its support for harmonising the enhanced due diligence measures to be taken towards operators in high-risk third countries. As regards the design of the future rules, while respondents in the private sector largely support the idea of harmonising EU AML/CFT rules and departing from the current minimum harmonisation approach, not least in order to ensure a level-playing field within the internal market, they stress the need to maintain a risk-based approach to avoid excessive burden on sectors less exposed to risks. Similarly, public authorities seem rather wary of excessive harmonisation in the field of supervision (including sanctioning powers) and regarding the tasks and powers of the FIUs.

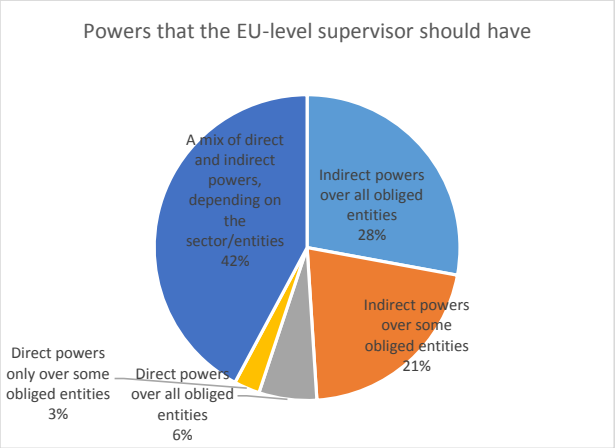
There is widespread support for better interaction between AML/CFT rules and other EU rules (in particular on exchange of information with prudential supervisors, consistency with the Payment Service Directive and the Payment Account Directive and introduction of strict AML/CFT requirements in fit & proper tests), although across respondent groups the level of familiarity with these rules varies (with NGOs, citizens and business associations outside the financial sector less likely to respond). Beyond the replies provided to the options put forward by the Commission, respondents widely demanded clarification of how AML/CFT rules interact with data protection rules, both in terms of facilitating exchanges of information (private sector) and of protecting privacy (NGOs).

Pillar 3 – EU-level supervision

The public consultation invited views on the options set out in the Action Plan regarding an EU-level AML supervisor.

As the chart shows, the majority of respondents (55%) consider that an EU-level supervisor should cover all obliged entities, although a relative majority (34%) prefer to achieve this gradually. Support for only covering financial institutions or credit institutions is lower (respectively 25% and 20%). Several entities in the non-financial sector oppose being subject to EU-level supervision, whether directly or indirectly, in light of their sectorial specificities. Conversely, operators in the financial sector consider that all entities should fall within the scope of the EU-level supervisor. Some respondents in the public sector commented that supervision by self-regulatory bodies in the non-financial sector has proven to be a failure.





In terms of powers, as the chart to the left shows, respondents oppose an EU supervisor that would directly supervise obliged entities (only 9% support this). Instead, there is wide support for a "supervisor of supervisors" who can intervene in justified cases (49%), or for a mix of powers, depending on the sector (42%). This view was shared across all stakeholder groups.

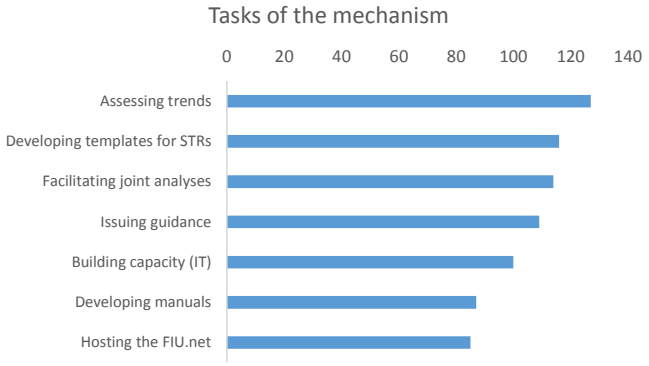
Most respondents were unable to indicate how to identify entities to be directly supervised by the EU-level supervisor. This reflects the opinion that supervision of the national supervisors should be prioritised. Respondents who had an opinion on this issue indicated that a risk-based approach is preferable to identifying the entities from the outset or national supervisors proposing them.

Finally, the consultation reveals low support for the European Banking Authority becoming the future EU AML/CFT supervisor. While one third of respondents did not express any opinion, only 19% of those who did supported the EBA. These respondents manly spoke for the non-financial sector, a fact underlying the opposition of operators in this sector to being covered by EU-level supervision. This option has however little support across all other respondent groups. 66% of respondents favour a new body, again with quite similar levels of support across all other respondent groups. Views are

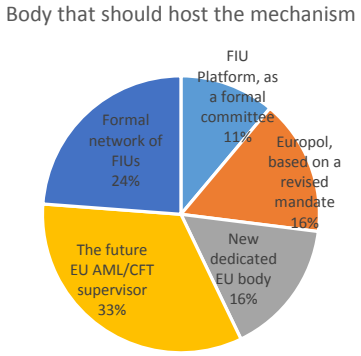
however split as to the structure that this body should have. Of those who replied "other" (essentially operator in the private sector), a few would favour the ECB taking over this task, despite the fact that the Treaty does not provide a legal basis for the ECB to perform AML/CFT supervision.

Pillar 4 – Support and coordination mechanism for Financial Intelligence Units

The public consultation invited views on the options set out in the Action Plan regarding the tasks of the FIU support and coordination mechanism and which body should host it.



Respondents across all stakeholder groups favour that the FIU support and coordination mechanism performs a broad array of tasks. The emphasis placed on assisting the analytical work of the FIUs rather than on the sole provision of IT tools confirms expectations that the mechanism will help FIUs produce better financial intelligence rather than just providing technical assistance.



Answers diverge on the form the mechanism should take and who should host it. Again, more than one third of respondents did not express a view on this, stressing the priority that content should take over form. The graph to the left shows the reactions of respondents who had an opinion on this issue, and indicates a preference for mechanism to be hosted by the EU AML supervisor. This option is clearly favoured by EU citizens and companies, while business associations and public authorities have their views split across the different options and NGOs favour a formal network of FIUs. Overall, the answers underscore that this mechanism will have to maintain a high level of autonomy for the FIUs.

5. Targeted consultations of Member States

The Commission discussed the topics analysed in this impact assessment during 4 meetings of the Expert Group on Money Laundering and Terrorist Financing held in May, June, September and October 2020, as well as during 2 meetings of the EU FIUs' Platform held in June and October 2020.

The discussions were supported by targeted consultations of Member States and competent authorities. The following supports were used:

- A questionnaire to compile Member States' experiences and views on the current legislative framework, the powers, scope and structure of the future EU supervisor, the tasks and structure of an FIU support and coordination mechanism, and public-private partnerships.
- A questionnaire to collect the latest data on the functioning of the current system.
- A questionnaire to assess experience with cross-border access to bank account information and a questionnaire to collect information on the authorities having access to centralised bank account registries.

These consultations confirmed many of the Commission findings regarding the functioning of the current system and need for reform. The input provided by Member States has been integrated throughout the impact assessment.

6. Consultation of the EBA

In March 2020, the Commission services requested advice from the EBA on the areas where AML/CFT rules could be strengthened. The EBA provided its opinion on 10 September.

The EBA recommended the Commission to harmonise aspects of the current EU AML/CFT framework where divergence of national rules has had a significant adverse impact, such as customer due diligence measures, internal control systems, supervisory risk assessments, cooperation and enforcement. The EBA further suggested to strengthen aspects of the EU's legal framework where vulnerabilities exist, such as in regard of the powers of AML/CFT supervisors and reporting requirements.

The EBA recommended to expand and clarify the list of obliged entities, in particular with regard to crypto asset service providers, investment firms and investment funds. It also suggested to clarify provisions in sectoral financial services legislation (in particular data protection, payment services, financial sanctions and deposit guarantee schemes) to ensure that they are compatible with the EU's AML/CFT objectives.

This input has been integrated throughout the impact assessment.

7. Opinion of the European Data Protection Supervisor

On 23 July, the EDPS issued an opinion on the Commission's Action Plan. In relation to the three reform pillars analysed in this impact assessment, the EDPS:

- Noted its support for harmonising the AML/CFT framework and maintaining a risk-based approach, also in line with the data protection principles.
- Suggested, in relation to EU-level supervision, to include a specific legal basis to process personal data and the necessary data protection safeguards, particularly regarding information sharing and international transfers of data.
- Welcomed the intention to find a suitable solution for the management of FIU.net in line with data protection and recommended clarifying the conditions for access to and sharing of information on financial transactions by FIUs.

The EDPS commented on possible areas for harmonisation interacting with data protection. These have been addressed in the analysis presented in this impact assessment.

8. High-level conference on the future of the AML/CFT framework

On 30 September, the Commission organised a high-level conference with three panel debates dealing with the three objectives for which this impact assessment analyses possible policy options. These panels brought together representatives from national and EU authorities, MEPs, private sector and civil society representatives and academia.

The panels concluded that:

- There is a need for more harmonised rules, as well as better information sharing.
- As regards EU-level supervision, while the financial sector is a priority, the non-financial sector also needs to be covered. In this area, supervision by self-regulatory bodies has not worked adequately. An EU supervisor should be an independent agency with the power to impose sanctions and responsible for supervising high-risk entities identified on the basis of an EU-wide risk assessment. This supervisor should work closely with national supervisors.
- FIUs need better tools to perform their work. The key challenge is understanding how criminals operate and while centralised reporting and production of financial intelligence at EU level would not work, joint analyses could significantly improve the detection of suspicious flows. This would improve work between FIUs and cooperation with reporting entities. Those entities in the non-financial sector are particularly exposed and may often act as enablers.

Two high-profile prosecutors took the floor as keynote speakers, focussing on the most urgent threats: uncapped cash payments, crowdfunding, crypto currencies and prepaid cards. They considered financial intelligence key to detecting criminal activities.

In their closing remarks, the Commission, Council and European Parliament committed to taking bold steps to protect the EU financial system from illicit money.

ANNEX 3: WHO IS AFFECTED AND HOW?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

The objective of this Annex is to set out the practical implications for stakeholders affected by this initiative, mainly businesses in the financial and non-financial sector (obliged entities), public administrations at the national and European level and citizens. The initiative aims to simultaneously achieve the following objectives:

- Objective 1: Strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards.
- Objective 2: Improve the effectiveness and consistency of anti-money laundering supervision.
- Objective 3: Increase the level of cooperation and exchange of information among Financial Intelligence Units.

In order to **strengthen EU anti-money laundering rules, enhance their clarity and ensure consistency with international standards** (Objective 1) the preferred option is to harmonise to a greater extent both the AML/CFT obligations for the relevant entities as well as the powers and obligations of supervisors and FIUs (Option 3). This would entail clarifying and restructuring existing rules that are applicable to obliged entities through a directly-applicable Regulation. It would not introduce major new rules, rather ensure their coherence and consistent application within the EU. Furthermore, it would add minimum common rules covering the performance of key supervisory tasks, covering operational aspects of cooperation among national AML supervisors and with an EU-level supervisor (set up under Objective 2). The powers of competent authorities would be clearly defined and made binding at EU-level, to ensure that they have equal powers across the EU.

A harmonized and consistent EU AML/CFT framework would benefit the obliged entities, both from the financial and non-financial sector. This would remove an uneven AML framework faced by entities operating in several Member States and would facilitate trading across the Internal Market. It would also decrease legal uncertainty and administrative burden (by lowering compliance costs) for such entities. In particular cross-border active SMEs among the obliged entities would benefit, as they are less able to bear large compliance costs. All obliged entities and public administrations would benefit from a coherent and consistent EU AML/CFT framework as it would eliminate opportunities for regulatory arbitrage.

Harmonization through a regulation of the substantive requirements contained in the AML Directive could entail initial higher compliance costs for some non-cross-border private entities, particularly those operating in jurisdictions with lower requirements thus far. However, these costs would be one-off and fairly limited; adjustments would be required in internal processes and procedures, but are not expected to generate a need for

significant investments in infrastructure or expensive technologies. Obliged entities in the financial sector would be most affected as they frequently operate across borders.

Greater harmonization would also benefit competent authorities by providing them with a framework to consistently apply AML/CFT rules across the EU. No competent authority is expected to be negatively affected, i.e. forced to adopt lower standards than currently in force nationally, as these rules would allow for a risk-based approach at national level, leaving scope for some national rules to go further where justified. Competent national authorities would be find it easier to cooperate across borders and detect cross-border AML/CFT transactions. This would also ensure smooth cooperation with an EU-level supervisor. These changes would bring additional adjustment costs in terms of human and financial resources initially, by these would be one-off and would swiftly be offset by benefits in terms of enhanced capacity and efficiency.

With regard to consumers/citizens, they should not be affected negatively by these changes.

In order to **improve the effectiveness and consistency of anti-money laundering supervision** (Objective 2) the preferred option is to supervise directly a selected number of entities at EU-level through an EU-level supervisor (Option 3). Initially the supervised entities would be cross-border financial groups. They would also carry most of the additional costs of EU-level supervision, for example, in fees paid to the supervisor. However, given that majority of these entities would be large and cross-border, the increased effectiveness and efficiency of supervision should outweigh these costs, as acknowledged by respondents to the public consultation.

The setting-up of an EU supervisor would also affect national competent authorities. Relevant national authorities would continue to supervise entities not directly supervised by the EU supervisor. The EU-level supervisor would lessen to some extent the workload, but not replace national authorities, as the majority of the financial sector obliged entities, and all non-financial obliged entities, remain under national supervision.

With regard to consumers/citizens they should not be affected negatively by these changes.

In order to **increase the level of cooperation and exchange of information among Financial Intelligence Units** (Objective 3) the preferred option is to provide the EU FIUs' Platform with power to issue guidelines and technical standards and to organize training and joint analyses, carry out trends and risk analysis (Option 3). The EU FIUs' Platform would become a formal Coordination and Support Mechanism of EU FIUs, in principle becoming part of the envisaged EU AML supervisor (foreseen under Objective 2). Secretariat staff in the FIU division of the agency would ensure the technical administration of FIU.net and facilitate coordination and work of the FIUs. Hosting of FIU.net is due to be carried out temporarily by the Commission from 2021.

National Financial Intelligence Units would also be positively affected by the development of common templates and methodologies. This would facilitate cooperation and over time lead to greater detection of cross-border money laundering/terrorism

financing. These efficiency gains will outweigh temporary costs associated with developing and implementing these new templates.

With regard to consumers/ citizens they should not be affected negatively by these changes.

2. SUMMARY OF COSTS AND BENEFITS

Increased effectiveness of AML/CFT rules, consistent supervision across the internal market and efficient exchange of information among FIUs is the main objective of the initiative. This should reduce the quantity of illicit funds which are laundered or used to finance terrorism, either through greater detection or deterrence.

Preferred Options:

- *Ensure a greater level of harmonisation in the rules that apply to entities subject to AML/ CFT obligations and the powers and obligations of supervisors and FIUs.*
- *Direct supervisory powers over selected risky entities in the financial sector subject to AML/ CFT requirements and indirect oversight over all other entities.*
- *The EU FIUs' Platform to become a mechanism as part of the AML Authority, with power to issue guidance and technical standards and to organise joint analyses and training, carry out trends and risk analysis.*

I. Overview of Benefits (total for all provisions) – Preferred Options		
Description	***Amount***	***Comments***
Direct benefits		
Harmonisation of rules that apply to entities subject to AML/ CFT obligations	A detailed and coherent rulebook for entities subject to AML/ CFT requirements across the EU Removal of barriers to the Internal Market Lower compliance costs for cross-border obliged entities Higher legal certainty	Businesses would benefit by the creation of a level playing field as regards rules and obligations applicable to entities subject to AML/ CFT requirements, i.e. CDD and BO obligations. Lower compliance costs over time, in particular for cross-border obliged entities Competent authorities would benefit from an enhanced capacity and more efficient execution of tasks
A consistent beneficial ownership (BO) transparency regime	Improved identification of beneficial owners across the EU	Citizens right to privacy would continue to be ensured through consistent rules on collection and storing of BO information in central registers and the existence of safeguards for accessing this information
Consistent powers and obligations of AML/ CFT supervisors across the EU	Removal of barriers to operating in the Internal Market Higher legal certainty	Supervisors would be granted a minimum set of powers. Such powers would be clear, binding at EU level and allow adequate exercise of supervision for all supervisors

		Obliged entities would benefit from a consistent definition of the criteria and thresholds for sanctions.
Consistent powers and obligations of FIUs	Better detection of cross-border suspicious transactions	
Direct supervision of selected entities by an EU supervisor and indirect oversight over all other entities	For directly supervised entities, especially cross-border groups, advantage of dealing with one single AML/CFT supervisor.	National supervisors would be relieved of the burden of supervising entities selected for direct EU supervision. Supervised entities would benefit from harmonised EU-level supervision, rather than being subject to divergent national approaches
Coordination and support of EU FIUs through the mechanism	Better information exchange on emerging AML/ CFT risks and trends. Higher level of expertise among staff in national FIUs thanks to intensified exchanges of practices and experiences.	FIUs would benefit from better information exchange by carrying out joint analyses and training. Strong support and coordination of national FIUs through a dedicated Secretariat.
Development of common reporting standards, templates and non-binding guidance	Facilitation and reduced cost of reporting.	Obliged entities benefit from improved feedback. FIUs benefit from better cooperation, more effective information flow, comparable data and operational capacity development through peer reviews.
Indirect benefits		
Greater cooperation among EU AML supervisors and other national competent authorities	Improved application of AML/CFT rules and greater detection of suspicious transactions	
Greater cooperation of EU AML supervisors and national competent authorities with designated EU supervisor		
Indirect supervision and coordination of national AML supervisors	More coherent and harmonised practices among national supervisors	Supervisors would benefit from greater coordination.
Development of common reporting standards and templates	Facilitation of cooperation among FIUs.	Cooperation with other competent (non-FIU) authorities enhanced.

II. Overview of costs – Preferred options						
	Citizens/Consumers		Businesses		Administrations	
	One-off	Recurrent	One-off	Recurrent	One-off	Recurrent

Harmonisation rules that apply to entities subject to AML/ CFT obligations	Direct costs			Adjustment costs to the new framework (esp. entities newly covered, and CASPs brought under Regulation 2015/847)		Adjustment costs through modification of procedures, tools and human resources	
	Indirect costs						
Direct supervision of selected entities by a designated EU supervisor	Direct costs				EU supervision funded through recurrent fees levied on supervised entities (total annua cost: approx. EUR 30 million)		
	Indirect costs					Potential movement of staff from national to a EU supervisor	
Coordination and support of EU FIUs through the mechanism	Direct costs					Setting up an FIU mechanism within the AML Authority	Operating an FIU mechanism within the AML Authority
	Indirect costs						

ANNEX 4: EVALUATION[74]

At the time of adoption of this impact assessment, a full evaluation of the fourth and fifth AML Directives had not yet taken place. The fourth AML Directive[75] was adopted on 20 May 2015, with a transposition deadline for Member States of 26 June 2017. The Fifth AML Directive[76] was adopted on 30 May 2018, with a transposition deadline of 10 January 2020. Major delays in transposition of both Directives in certain Member States led to the opening of infringement procedures for non-notification or incomplete notification. At the date of this impact assessment, while complete notifications have been received from all Member States for the 4th AMLD, that is not the case regarding the 5th AMLD, and for both Directives, completeness and conformity assessment of the transposition notifications is still being carried out by Commission services.

Article 65 of the consolidated AML Directive obliges the Commission to submit a report to the European Parliament and the Council by 11 January 2022 (two years after the transposition deadline of the 5th AMLD), and every three years thereafter, covering a number of elements[77]. In pursuance of the preparation of that report, the Commission has

[74] This Annex should be read in conjunction with section 7 in the Impact Assessment, where effectiveness efficiency and coherence of the proposal are considered.

[75] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[76] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

[77] AMLD, article 65.1: "By 11 January 2022, and every three years thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and to the Council.

That report shall include in particular:

(a) an account of specific measures adopted and mechanisms set up at Union and Member State level to prevent and address emerging problems and new developments presenting a threat to the Union financial system;

(b) follow-up actions undertaken at Union and Member State level on the basis of concerns brought to their attention, including complaints relating to national laws hampering the supervisory and investigative powers of competent authorities and self-regulatory bodies;

(c) an account of the availability of relevant information for the competent authorities and FIUs of the Member States, for the prevention of the use of the financial system for the purposes of money laundering and terrorist financing;

(d) an account of the international cooperation and information exchange between competent authorities and FIUs;

(e) an account of necessary Commission actions to verify that Member States take action in compliance with this Directive and to assess emerging problems and new developments in the Member States;

(f) an analysis of feasibility of specific measures and mechanisms at Union and Member State level on the possibilities to collect and access the beneficial ownership information of corporate and other legal entities incorporated outside of the Union and of the proportionality of the measures referred to in point (b) of Article 20;

(g) an evaluation of how fundamental rights and principles recognised by the Charter of Fundamental Rights of the European Union have been respected."

entrusted the Council of Europe with submitting reports on the application and enforcement of EU AML rules in each of the Member States; those reports will be received in the course of 2021, with the last ones possibly only received in 2022 (the timetable will be affected by the COVID-19 pandemic).

Regarding the envisaged relevance, EU added value and coherence of 4th and 5th AMLD, reference is made to the impact assessments accompanying the proposals of those Directives[78]. In particular, during the preparation of the 4th AMLD, coherence with the following EU policies and priorities was taken into account: the Internal Security Strategy, the Commission proposal on data protection which became GDPR, and the Commission policy on sanctions and on financial inclusion. The 5th AMLD made targeted amendments to the 4th AMLD in order to fill certain gaps which were identified in the meantime, for example adding certain Obliged Entities and creating an interconnection between registers of Beneficial Ownership.

The urgency of proceeding with a new initiative in the area of AML/CFT, before full evaluation of the 4th and 5th AMLD is completed, is explained in the Commission's Action Plan of 7 May 2020, and the background is described in the package of Commission documents adopted in July 2019[79]. These documents, adopted after the transposition deadline of AMLD4 but not that of AMLD5, deal with the effectiveness and efficiency of the EU AML/CFT regime as it stood at that time, and can be considered as constituting a preliminary evaluation of the regime.

The effectiveness of the existing AML regime in reducing the amount of ML can only be indirectly perceived via proxy indicators, such as the number of instances of ML which come to light; as with any system for detecting and reducing crime, such an indicator can be misleading, since an improvement in the regime can lead to more cases coming to light, which would previously have remained undetected. Moreover, AMLD4 and AMLD5 have not been implemented for long enough for a meaningful set of data to be available.

Efficiency, on the other hand, can be assessed using indicators such as the volume of communication and cooperation between relevant authorities, both domestically and cross-border, the quality and quantity of reporting from Obliged Entities and feedback received. The 2019 "post-mortem" report highlights insufficiencies in these areas, including defensive over-reporting by OEs, leading to the "false positives" referred to in section 2.1. of the impact assessment. The future Authority will have a central role to play in promoting more efficient enforcement practices.

The 2019 package consisted of a Communication entitled "Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework" accompanied by four reports:

[78] SWD(2013)21 final of 5 February 2013, and SWD(2016)223 final of 5 July 2016.
[79] See footnote 4.

- Report assessing recent alleged money-laundering cases involving EU credit institutions (the "post-mortem report").
- Report assessing the framework for Financial Intelligence Units' (FIUs) cooperation with third countries and obstacles and opportunities to enhance cooperation between Financial Intelligence Units within the EU.
- Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union;
- Report assessing the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of central bank account registers and data retrieval system (see annex 7).

The "post-mortem report" drew on facts from case studies covering a sample of ten public cases involving credit institutions during the period 2012-2018. It assesses the role of the credit institutions, and the powers and actions of the anti-money laundering/countering financing of terrorism and prudential supervisors. The analysis of the selected cases revealed substantial incidents of failures by credit institutions to comply with core requirements of the Anti-Money Laundering Directive, such as risk assessment, customer due diligence, and reporting of suspicious transactions and activities to Financial Intelligence Units. In some cases, supervisors only intervened after significant risks had materialised or in the face of repeated compliance and governance failures.

The report on Financial Intelligence Units showed that some FIUs failed to engage in a meaningful dialogue with obliged entities by giving quality feedback on suspicious transaction reports. The lack of templates for reporting also hampered the quality of the reports by obliged entities.

The Communication concluded that "whereas many risks and shortcomings have already been or will shortly be addressed thanks to the recent changes in the regulatory framework, some of the shortcomings identified are structural in their nature and have not yet been addressed."

These reports thus showed failings in the effectiveness and efficiency of the EU AML system, stemming from all three key components: Obliged Entities, supervisors and FIUs, and the interaction between those entities.

Building on the documents in the package of July 2019, the Action Plan of May 2020 committed the Commission to take further action to strengthen the AML/CFT framework of the EU, certain of which require further legislation, in particular a single EU rulebook, EU-level supervision, and a support and cooperation mechanism for Financial Intelligence Units.

Regarding the single rulebook, the Action Plan noted that the current approach to EU legislation has resulted in diverging implementation of the framework across Member States and that lack of detail in the applicable rules and on the division of responsibilities

with regard to cross-border issues results in differing interpretations of the Directive across Member States. It considered that to limit divergences in the interpretation and application of the rules, certain parts of the AMLD should be turned into directly applicable provisions set out in a Regulation.

With regard to a single EU supervisor, the Action Plan found that the Union does not have in place sufficiently effective arrangements to handle AML/CFT incidents involving cross-border aspects. Against this background, it concluded that there is a clear and evidenced need to have in place an integrated AML/CFT supervisory system at EU level that ensures consistent high-quality application of the AML/CFT rulebook throughout the EU and promotes efficient cooperation between all relevant competent authorities.

Regarding FIUs, the Action Plan identified a number of weaknesses with respect to how FIUs apply the rules and cooperate between themselves and with other authorities at domestic level and across the EU. Domestically, the use of templates for reporting by obliged entities is still limited, and these are often tailored to the needs of specific businesses (e.g. banks). Several FIUs still lack the necessary IT tools to effectively process and analyse the information. Feedback from FIUs to obliged entities in relation to their reporting remains limited. The limited information exchange between FIUs and other competent authorities is of great concern. For these reasons, the Action Plan found that an FIU coordination and support mechanism at EU level should be created and take a leading role to coordinate the work of national FIUs. This should include identification of suspicious transactions with a cross-border dimension, joint analysis of cross-border cases, identification of trends and factors relevant to assessing the risks of money laundering and terrorist financing at national and supranational level. The mechanism should also coordinate FIUs' activities, cooperation and templates, as well as promote training and capacity building for FIUs. It should also enhance cooperation among competent authorities (FIUs, supervisors, law enforcement and customs and tax authorities), both domestically and across borders, and with FIUs from outside the EU.

The public consultation launched by the Action Plan, and described in Annex 1 above, revealed broad support for these actions.

ANNEX 5: EU AML AUTHORITY: ORGANISATIONAL INSTITUTIONAL, RESOURCE AND BUDGET ISSUES

1. Institutional options for implementation of the reform

The institutional reform presented by the options selected in the impact assessment has two dimensions:

- A single Union AML supervisor with either direct or indirect supervisory powers over all obliged entities subject to AMLD plus regulatory powers in certain areas.
- An FIU support and coordination mechanism, with powers to, *inter alia*, adopt binding templates to be used by FIUs, facilitate joint analyses and host FIU.net.

The functions of supervision and financial intelligence are distinct, although certain Member States combine them into a single authority, enabling more expedient interaction and information exchange (which, as explained in the main body of this impact assessment, is critical for the effective implementation of the AML/CFT framework). Given these different possible models, it is necessary to consider options both for combining these two functions, or locating them separately; in both cases, this could be either as a new entity or as part of an existing EU institution or agency.

1.1.Options for distribution of new tasks to existing bodies

a) *Supervision function: option of extending EBA mandate*

The European Banking Authority already has certain indirect supervisory powers in the area of AML applicable to financial sector entities. Direct supervisory powers for financial sector entities could at first sight be seen as a logical extension of its current mandate. However, difficulties have been encountered with regard to exercising some of EBA's current powers, especially those related to enforcement, due to specificities of the EBA governance model. Direct supervisory powers over obliged entities would also require a different governance model for effective and efficient functioning of direct Union-level supervision, given the new types of decisions vis-à-vis obliged entities that would need to be taken in an efficient and expedient manner. Therefore, EBA would need to have a dual decision-making model – one for existing functions other than AML, and another for AML tasks only. Moreover, EBA has no experience with direct supervision of entities in the financial sector, and would need to build that expertise.

Next, the scope of EBA competence is currently limited to the financial sector. Indirect supervision powers related to the non-financial sector as well as regulatory and policy tasks (including High-Risk Third Countries) that concern the entire universe of obliged entities cannot therefore be viewed as an extension of its current mandate and would require a new mandate extending far outside the financial sector. The combination of all additional tasks would dwarf the current tasks and powers in the area of AML, and make

EBA a huge and hybrid entity. Coupled with the required parallel governance structure, the disadvantages in terms of additional costs attached to this option would outweigh any of its benefits related to leveraging an existing agency's resources, infrastructure and expertise.

Furthermore, a majority of stakeholders from both private and public sector in public consultations conducted by the Commission voiced their preference for a new Union body to be granted these powers, as opposed to the EBA (see annex 2).

Therefore, this option for supervision, while legally feasible, is deemed not optimal.

b) *FIU support coordination mechanism: options for siting in existing bodies*

The FIU mechanism should combine new powers related to coordination of the national FIUs (including regulatory powers for issuing binding templates), which are an entirely new type of powers at EU level. It is necessary to examine whether either Europol or the Commission could potentially integrate the new FIU coordination mechanism, and the hosting of FIU.net.[80]

Europol's role is related to prevention and combatting of serious cross-border crime and is defined in Article 88 TFEU as "to support and strengthen action by the Member States' police authorities and other law enforcement services (…)". The Europol Regulation[81] is currently being amended, with the potential for extension of its current role. However, FIUs are not law enforcement agencies, and despite the fact that they are sometimes integrated in law enforcement agencies, the tasks relating to support and coordination of FIUs covers a pre-criminal phase. Therefore, this task falls outside the Treaty competence of Europol under Article 88 TFEU, even if its Regulation were to be amended[82].

With regard to the Commission, the Commission permanently taking the role of the FIU coordination mechanism as described in section 5 of the Impact Assessment would infringe the principle of FIU operational independence enshrined in the AML Directive and reflecting FATF standards on FIUs[83], as under the auspices of the Commission, the Commission itself would take decisions, aided only by a comitology committee, as described in option 2, which was deemed sub-optimal.

Therefore, no existing body could host the FIU coordination mechanism**.** Moreover, in the public consultation, a majority of stakeholders, including FIUs, voiced their

[80] FIU.net is currently hosted by Europol, but being temporarily transferred to the European Commission due to an EDPS decision based on limitations in the personal data that Europol can process under its current Regulation. See footnotes 48 and 61 above.
[81] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation.
[82] It should however be noted that Europol has nevertheless expressed a desire to be the seat of any future Cooperation and Support Mechanism for FIUs (letter to European Commission of 21 October 2020).
[83] FATF Recommendation 29 on FIUs and interpretative notes, and AMLD article 32, "*Each FIU shall be operationally independent and autonomous*".

preference for a new Union body or the future EU-level AML supervisor to carry out the functions of the FIU support and coordination mechanism.

In conclusion, distributing the new tasks among existing bodies is not a viable option.

1.2. Location of both new functions in a new EU AML Authority

Given the unsuitability of existing EU entities to host the EU AML supervisor or the FIU coordination mechanism, the only remaining option is the creation of a new agency to do this. While theoretically it might be conceivable to create such two new agencies, one for the EU supervisor, and one for the FIU coordination mechanism, combining them can produce large cost savings compared with two agencies, and some synergies can be anticipated. Indeed, in certain Member States these functions are combined in a single entity. Furthermore, having one AML Authority at Union level bringing under the same institutional umbrella different stages for countering effectively money laundering and terrorist financing seems the only policy response that can account for the call for a comprehensive EU AML/CFT policy.

At the EU level, the functions of supervision and that of coordination and support of the work of national FIUs will be distinct as at national level, but their close interaction will be even more important than at the national level because of the Union-wide implications of their work. Binding regulatory products and supervisory guidance that would be addressed to all obliged entities should be based on the risks and trends identified at Union level, and they should be supported by supervisory insights as well as information disseminated by FIUs, or derived from the joint analyses conducted by FIUs (and coordinated at EU level). Development of policy regarding HRTCs or regulatory measures also necessitates input from both supervision and FIUs coordination functions.

2. Resources and governance of a new Authority

For the reasons given above, the chosen option assessed here from a budgetary perspective is the establishment of a single new agency that would combine both a single Union AML supervisor and an FIU support and coordination mechanism – EU AML Authority (AMLA).

As a preliminary remark, a large part of the cost of a new Authority, the part linked directly to staff numbers, would be the same regardless of whether it is a separate new Agency or integrated into existing Agencies or other bodies. Only the start-up costs and the central administration functions of a new Agency would be saved by integrating the new functions into an existing body. It would take three years from the date of starting operations for the Authority to reach its full staffing level.

Governance and organisation

The organisational structure could follow the so-called ‘hub and spoke’ model, with:

- A central level, involving participation of national supervisors and FIUs and which would be supported by a secretariat with key tasks.
- A decentralised delivery of supervisory activities and of financial intelligence (including some staff members, including heads of direct supervision teams, permanently based in Member States).

Regarding decision-making, the vast majority of the decisions of the Authority could be taken by a small Executive Board of independent members who are not heads of any national supervisor or FIU. Regulatory decisions (including binding standards or templates for FIUs) would be adopted by a General Board, on which all Member States would be represented, which could meet in two different compositions (heads of national supervisory authorities or FIUs depending on the type of decision).

Funding and human resources needs

Staffing levels would depend on the number of entities supervised directly, as each such entity would require at least two staff members (bearing in mind that only the riskiest entities would be supervised at EU level, and also that for those entities, national supervisors would also contribute members of the supervision team). Functions other than direct supervision would require about 150 permanent staff (comparable to individual ESAs), and a limited number of directly supervised entities would require about 100 more, making a total of 250. Such a staffing level would generate an annual budget at a steady state of approximately EUR 42 million (including employer's pension contributions).

Funding would come from a combination of fees levied on certain Obliged Entities and a contribution from the EU budget, depending on the tasks and functions.

Functions financed by fees from obliged entities

Following the prevalent practice at national level and in the SSM, direct and indirect supervision of the financial sector should be financed via fees. Based on the estimate above, that would amount to 50% to 70% of the budget of the Authority (EUR 21 million to EUR 29 million) covered by supervisory fees. Since the selection of the entities for direct supervision would be risk-based, both directly supervised entities as well as entities that are in the same risk bracket and close to meeting other criteria for selection should contribute to supporting the supervision function. A broad distribution of fees is necessary because risky entities that are not selected for direct supervision would still benefit from a high degree of supervisory attention, including from the EU Authority. This corresponds to a wider pool of entities with a similar risk level which are liable to fall under direct supervision. Proportionality can be ensured by requiring smaller contributions from indirectly supervised entities of the same size, plus correcting the amounts for size and complexity.

A Delegated Regulation would lay down the exact methodology for calculation and distribution of fees. For comparison, the prevalent practice in the case of the Single Supervisory Mechanism for banks (SSM) is financing of direct supervision by the

supervised entities. In addition, in the case of the SSM, certain indirectly supervised entities (some categories of less significant institutions) also pay a fee, albeit with proportionately smaller amounts. The amounts of fees are determined by the ECB itself based on incurred costs, and their distribution among supervised entities is based on the size and risk exposure of the entity.

Functions financed by contribution from Union budget

The other functions (including FIU coordination mechanism, indirect supervision of the non-financial sector, policy functions) should be financed by a contribution from the Union budget. The nature of these tasks is akin to the tasks that are publicly funded at EU level already (i.e. regulatory and policy-making tasks similar to those currently carried out by the European Supervisory Authorities), or are publicly funded at national level (such as the functioning of the FIUs). These tasks carry benefits beyond the scope of entities susceptible to be covered by direct supervision. Thus, levying fees for these purposes is questionable as regards both the reasonable burden imposed on directly supervised entities and the prejudice that such private funding might bring to carrying out these tasks in the public interest. In addition, levying fees for indirect supervision of the non-financial sector entities, and of the financial sector entities that are unlikely to be directly supervised at EU level would constitute an additional financial burden on these obliged entities that cannot be justified by calculable and individual added value on top of the benefits deriving from national supervision.

ANNEX 6: AREAS FOR GREATER HARMONISATION OF RULES

1. **Introduction**

The AMLD is a minimum harmonisation legal framework. Pursuant to its Article 5*: "Member States may adopt or retain in force stricter provisions"* in the AML/CFT field. A minimum harmonisation framework has been necessary to accommodate pre-existing different national approaches, the relationship to national criminal law, and to facilitate a flexible response to specific local ML/TF risks in direct application of the principle that preventing money laundering and terrorist financing must be risk-sensitive.

The majority of the provisions of the AMLD have been transposed faithfully in directly applicable national rules. However, Member States have adopted additional or more stringent rules in a number of areas. While this caters for the need to make EU provisions applicable at national level, it might also result in divergent frameworks that create obstacles to the application of the Union legal framework, as shown by examples quoted in this impact assessment.

These divergences can be removed either by harmonising Union law via incorporating the added elements, or by introducing more specific provision in Union law that reduce those divergences that have had a significant adverse impact.

However, in line with international standards, such a framework will need to retain flexibility and discretion, in particular where it is necessary to address ML/TF risks and vulnerabilities specific to a certain sector or jurisdiction. Further harmonised Union AML/CFT rules may allow Member States to adopt, in specific, well-reasoned and notified cases, rules that supplement the Union framework with permanent or temporary measures.

As proposed by the European Banking Authority in its Advice to the Commission, the guiding principles deciding the building blocks of the single rulebook should be the following:

- The legal framework is proportionate and risk- sensitive, in line with international standards;
- New, or more detailed, rules should be introduced only where there is evidence to suggest that the current approach has not led to reliably effective outcomes, and that similar results cannot be achieved through other means.
- More harmonised rules should be introduced where evidence suggests that divergences among Member States have a significant, adverse impact on the prevention of the use of the EU's financial system for ML/TF purposes.
- The future framework should ensure consistency of norms and supervision across the different sectors subject to AML/CFT requirements, without these rules being necessarily the same. No amendments should lead to a weakening of European or national AML/CFT standards;
- The future AML/CFT framework should underpin and facilitate the establishment and operations of the Union AML/CFT supervisor and the FIU coordination and support mechanism;

- In order not to overburden the generally applicable legal framework, empowerments for the adoption of delegated and implementing acts should be favoured for detailed rules.

2. **Obliged entities**

The AMLD identifies a range of entities that are required to apply AML/CFT rules, while allowing a margin for national appreciation to extend these requirements to additional professions and categories of undertakings. Almost all Member States have made use of this margin; consequently, in respect of some categories of undertakings, no level playing field exists in respect of their AML/CFT obligations. Examples include owners, operators or brokers of race horses; leasing intermediaries; postal operators; bailiffs; wholesalers; individuals involved in public procurement; pawnshops; trade unions and professional organisations; traders in debt; mergers and acquisitions or equity and business consultants and insolvency administrators. Some Member States also consider that the inclusion of some financial institutions within the scope of the AMLD is disproportionate.

There have been instances where Member States indicated that the set of entities subject to AML/CFT rules under their national framework is too broad and needs reviewing. On the other hand, there is evidence that the level of threat associated with operators assisting in the acquisition of citizenship or residence schemes is significant at Union level, without them being subject to AML/CFT requirements on this ground.

In its Advice to the Commission, the European Banking Authority refers to the following entities whose status under the AML rules requires clarification:

- **crowdfunding service providers:** In 2018, about 800 crowdfunding platforms were recorded in the EU[84]. This number is increasing steadily as alternative finance instruments become more popular. However, crowdfunding platforms are exposed to money laundering risks linked to frauds, and carry a risk that the money raised may be used to finance terrorist activities. EU rules on crowdfunding subject some of these platforms to a number of requirements to mitigate those risks, and provides for a report to be issued by 2023 to assess the need to include crowdfunding platforms among AML obliged entities[85]. The EBA recommends anticipating such mandatory assessment Inclusion of crowdfunding platforms as Obliged Entities seems justified, given that one third of Member States already impose AML/CFT requirements on crowdfunding service providers or are currently in the process of doing so and any backtracking on this, irrespective of the grounds that led Member States to such a choice, could result in a lowering of EU AML/CFT protection. The status quo is also not satisfactory as it would perpetuate the uneven application of AML/CFT rules to the same type of entities depending on where they are located in the internal market, with the risk of regulatory shopping – particularly for remote services such as this –

[84] K. Wenzlaff et al. (2020), "Crowdfunding in Europe: Between Fragmentation and Harmonization", *Advances in Crowdfunding,* pp 373-390. About 90 such platforms were located in the UK.
[85] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business

already highlighted in the Action Plan of 7 May. However, it does not seem proportionate to subject those crowdfunding platform that are subject to the Union Crowdfunding Regulation to full AML/CFT rules, until evidence of the effects of that regulation is gathered. For this reason, it seems more appropriate to limit ML/TF risks to which crowdfunding platforms are exposed and to ensure a level-playing field across the Union by imposing AML/CFT requirements on those crowdfunding platforms that are not subject to Union crowdfunding rules.

- **investment firms and investment funds:** The EBA recommends clarifying which of these entities in the investment sector should be subjected to AML/CFT requirements, and to align the terminology used in AML/CFT rules with that used in sector investment legislation. Such recommendation would ensure a level playing field by clarifying the scope of entities in the investment sector subject to AML/CFT requirements. The only alternative would be the status quo, which the EBA has assessed as sub-optimal in that it lacks the necessary clarity.

- **(non- life) general insurers and general insurance intermediaries:** The ML/TF risk associated with the activities of general insurers and intermediaries is in most cases limited, as recognised by the Commission itself in its 2019 SNRA. In its opinion, the EBA suggested looking into the opportunity of including such sectors under the AML/CFT framework as the system in place to comply with sanctions obligations could form a basis for compliance with AML/CFT requirements. However, the report does not provide a compelling reason for extending the scope of obliged entities in the insurance sector. Given the lack of any evidence for subjecting general insurers to AML/CFT rules, including at international level, it would not be proportionate to do so. In this area, the status quo, i.e. covering life and other investment-related insurances, seems the more appropriate approach.

- **mortgage credit intermediaries and consumer credit providers** that are not financial institutions, are not currently subject to AML/CFT obligations at EU level, but this is the case in certain Member States. Depending on their business model, consumer credit providers are exposed to different risks. This was reflected in the 2019 SNRA, which assessed the level of threat of terrorist financing for the consumer credit sector as 'significant'. The mortgage credit sector was similarly assessed as being exposed to 'significant' money laundering threats. Therefore, the current situation appears not to adequately protect the EU's financial system while also failing to deliver a level playing field. Instead, the approach proposed by the EBA to include mortgage credit intermediaries and consumer credit providers regardless of whether they are licenced as credit or financial institutions seems justified as it would, on the one hand, ensure an adequate level of protection of these service providers and, on the other hand, achieve a level-playing field in the sector.

- **account information service providers** are currently covered by the AMLD, although they are not involved in the payment chain and do not hold customer funds. Their inherent ML/TF risk is therefore very limited. This has led some Member States to conclude that these entities should not be covered by AML/CFT requirements. However, given the need to harmonise customer due diligence measures, and the fact that such harmonisation will allow to instil a higher degree of proportionality than

some Member States currently allow, it seems appropriate to ollow the EBA's suggestion that AISP should continue to remain within the scope of the AMLD. The alternative option, i.e. removing them from the scope of AML/CFT rules, does not seem justified in the face of the limited checks they would be asked to run and the fast developments in the sector, which could lead to an integrated provision of different types of services.

Given the wide range of entities covered by AML/CFT obligations across the EU, the best approach could be to include specific provisions for expanding the list of entities subject to AML/CFT rules. Whenever Member States consider that there is an evidenced need to cover additional sectors, this should be subject to an assessment by the Commission as to 1) whether this is justified and proportionate and 2) whether the level of risk rather justifies that the sector be subject to AML/CFT rules EU-wide.

One category of Obliged Entity is proposed for removal from the scope of AMLD in the present package of proposals, namely traders in goods, which are currently obliged to submit reports for large cash transactions above EUR 10 000[86]. The proposal to prohibit cash operations above EUR 10 000, described in Annex IX below, removes any rationale for the inclusion of traders in goods in the scope of AMLD, and permits an element of simplification of the EU AML regime.

3. **Customer Due Diligence measures**

The AMLD requires obliged entities to carry out customer due diligence (CDD) to identify and verify their customers' and their beneficial owners' identity on the basis of documents, data or information obtained from a reliable and independent source; to assess information on the purpose and intended nature of the business relationship; and to conduct ongoing monitoring of the business relationship.

CDD is central to AML/CFT efforts. Provisions in the AMLD are high level to facilitate the adjustment of CDD measures by financial institutions on a risk- sensitive basis. Yet, lack of sufficient detail on how obliged entities should assess the risk associated with a business relationship or transaction and on the intensity of the CDD required with regard to specific customer/transactions have led to divergent expectations by obliged entities. When more detailed rules have been adopted at national level, this has sometimes resulted in regulatory arbitrage, hampering the cross- border provision of financial services.

The EBA found that limiting the flexibility embedded in the EU's AML/CFT framework had a significant detrimental effect on the quality of some financial institutions' AML/CFT efforts. Feedback from competent authorities obtained in the context of the ESAs' 2019 Joint Opinion on ML/TF risks affecting the EU's financial sector suggests that some financial institutions have established themselves in Member States whose CDD requirements they perceived to be the most permissive, to make use of the freedom to provide services from that Member State to customers in other Member States. This appears to be of particular concern in the payments and e- money sectors. The EBA recommends harmonising the AMLD's CDD requirements with a view to achieving

[86] As noted in section 2.2.1. of this Impact Assessment, this obligation has not produced the desired results.

consistent, and consistently effective, CDD practices in Member States and across the Single Market.

In line with this, the revised framework should focus on ensuring a high degree of harmonisation of customer due diligence measures by:

- Making it explicit that the purpose of CDD measures is to obtain a sufficient understanding of the customer and risks, whilst also avoiding that CDD is used for commercial purposes.
- Setting out clearer criteria for determining the nature and type of CDD measures that are commensurate with different levels of ML/TF risk.
- clarifying the technologically neutral approach and the possibility to perform CDD remotely to overcome current barriers to the use of technological solutions for CDD purposes in some national frameworks. This approach will complement the guidance currently being requested of the EBA on this issue.

The weaknesses of the alternative approach (i.e. *status quo*) have been described at length in the problem definition, and make a compelling case for harmonisation of CDD at EU level.

4. **Occasional transaction CDD threshold**

The AMLD sets the CDD threshold for occasional transactions that are not transfers of funds at EUR 15 000. Some Member States have assessed the ML/TF risk associated with this threshold as significant and made use of their powers under Article 5 of the AMLD to reduce that threshold, at times significantly. In line with the findings of the SNRA and with the EBA recommendations, the future framework should sets out:

- a definition of the terms 'occasional transaction' and 'linked transactions" on the basis of the terms in the ESAs' Risk Factors Guidelines and Guidelines;
- a single CDD threshold for occasional transactions to reduce regulatory arbitrage.

These recommendations have been largely taken on board, although given the technical nature of these rules the resort to regulatory technical standards is at times preferred. As regards the definition of 'occasional transaction', there was no sufficient evidence in support of a need to define it except for specific cases in the financial sector which could be addressed otherwise (e.g. by clarification via technical requirements).

5. **AML/CFT systems and controls requirements**

The AMLD refers in high- level terms to the AML/CFT policies, controls and procedures that entities subject to AML/CFT rules should have in place to assess, mitigate and manage effectively the ML/TF risks that they have identified. AML/CFT systems and controls are risk- based and form an integral part of an institution's wider governance and internal controls framework. A number of Member States and competent authorities have taken a narrow view of such obligations.

In line with EBA recommendations, the proposal aims to ensure that rules regarding AML systems and controls:

- Are comprehensive, risk- sensitive, and proportionate to the nature, complexity and size of an entity;
- When the size of the entity justifies it, include a requirement to allocate to a member of the management body ultimate responsibility for the entity's AML/CFT systems and controls;

- Include a requirement to directly to report to the supervisory function of the board cases of significant or material weaknesses;
- Set out rules delineating responsibility for the oversight and enforcement of AML/CFT systems and controls requirements on the one hand, and wider governance requirements.

In this case as well the alternative (i.e. *the status quo*) does not seem appropriate. Even in a situation of further, yet not full, harmonisation of such requirements, the implementation of group-wide requirements would be particularly difficult, and the current situation combining high costs with ineffective systems would be perpetuated.

6. **Cooperation among authorities**

The AMLD requires Member States to ensure that AML/CFT supervisors of the home and host Member State cooperate to ensure effective AML/CFT supervision of cross-border financial institutions, but also domestically. Unlike provisions in some sectoral legislation, the AMLD does not create an explicit legal duty for all competent authorities to cooperate with each other, and with other stakeholders, by setting out the situations when this must take place. EBA has found that information exchange between supervisors, and between supervisors and FIUs, is often inadequate. Bilateral exchanges between FIUs and supervisors remain very limited in some Member States. As presented in the impact assessment, a similar problem exists as a result of a lack of obligation to cooperate for FIUs and customs authorities in relation to cash declarations.

In line with EBA recommendations and weaknesses detected, the preferred option includes:

- setting out an explicit legal duty for AML/CFT supervisors, prudential supervisors, FIUs, the Union AML Authority and other relevant authorities, including customs and tax authorities, to cooperate;
- creating a legal basis for the establishment of AML colleges, on the basis of the mandates for prudential colleges included in the Capital Requirements Directive (CRD).

As to alternative options, the only real alternative could be to leave these measures to be introduced at national level or based on voluntary initiatives (i.e. *status quo*). However, the cross-border nature of such cooperation, coupled with the need to ensure consistency in supervisory approaches, suggest that action at Union level would be more effective and likely to lead to better and more consistent outcomes.

7. **Sanctions**

The AMLD requires Member States to ensure that obliged entities can be held liable for breaches of national provisions transposing the AMLD, also laying down a list of minimum administrative measures that Member States have to be able to apply, unless they put in place criminal sanctions for the same breaches.

However, there is no consistent approach as regards investigating AML breaches and applying sanctions, and no common understanding, among supervisors, of what constitutes a 'serious' breach. A similar breach by a financial institution is therefore likely to trigger the imposition of different sanctions and measures, depending on which

supervisor is responsible for taking enforcement action, or no sanctions or measures at all.

Following the EBA advice, the preferred option strengthens the legal framework to include common criteria for defining a consistent approach to determining the gravity of the breaches identified. This will facilitate the mandate and operation of the Union AML Authority, enabling it to exert supervisory powers over individual obliged entities. To take account of different national systems, it seems appropriate to introduce the above measures whilst leaving Member States some margin on how to achieve them.

The alternative option would be the *status quo*, which consists of very different outcomes according to a supervisor's specific preference and powers. This does not appear adequate to ensure consistent protection of the Union's financial system.

8. **Crypto asset service providers (CASPs)**

CASPs are providers engaged in exchange services between crypto currencies and fiat funds, and crypto currency custodian wallet providers. They have been recently identified by the FATF as entities that should be subjected to AML/CFT rules, and the regulation of their service provision has been ensured through the Commission's recently-adopted Digital Finance Package of 24 September. Particular attention to coherence is therefore needed with regard to CASPs.

The new standards adopted by the FATF in October 2018 introduced a new definition of crypto asset, which is broader than the AMLD definition of crypto currencies[87]." The definition of 'virtual asset service providers' adopted by FATF is also broader than the AMLD's current definition. Union law should therefore be aligned with the FATF Standards, which will require to (1) broaden the AMLD's scope to crypto-assets activities not yet covered, (2) adapt the definition of crypto assets in use in EU AML/CFT legislation, (3) complete and review licensing and registration obligations for these obliged entities (4), modify the fit and proper tests to which senior managers of crypto assets providers are already submitted under AMLD5.

A further necessary alignment with the FATF standards consists in introducing into EU legislation the information sharing obligations contained in the so called "travel rule" contained in the Interpretative note to recommendation 15 of the FATF.

The new Commission proposal for a regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/193 (the MICA draft proposal) already provides:

(1) a **definition of 'crypto-asset service'** (in its article 3) which covers a list of services and activities to crypto-asset that reflects adequately the complete set of activities covered by the new FATF standards;

[87] FATF defines virtual assets as "'a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'

(2) a **definition of 'crypto-asset'**, defined as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology";
(3) **licensing and registration obligations for these different type of crypto-assets services providers**. Thus, Crypto-asset services should only be provided by legal entities that have a registered office in a Member State and that have been authorised as a crypto-asset service provider by the competent authority of the Member State where their registered office is located.
(4) **fit and proper test requirements for senior managers**: thus, the draft regulation provides that both Issuers of asset-referenced tokens and Crypto-asset service providers managers and main shareholders should be fit and proper for the purpose of anti-money laundering and combatting the financing of terrorism.

All four of these issues being already at least partially addressed in the future MICA regulation, it should be possible to address them for AML/CFT purposes through cross references in the future AML legislation.

The FATF has also adopted a "travel rule" for CASPs analogous to that for other fund transfers[88]. These requirements replicate for crypto assets service providers the obligations already in place in relation to cross-border wire transfers of funds of financial institutions. These rules have already been implemented in the EU by Regulation 2015/847 on information accompanying transfers of funds (Wire Transfer Regulation). Therefore, the easiest option to introduce the travel rule into EU law would be to modify the transfer of funds regulation to also encompass transfers of crypto assets. Similar safeguards regarding data protection would be introduced in that Regulation for crypto assets transfers as currently exist for other transfers[89].

The only alternative to introduce these rules would be the *status quo*. However, this would not mitigate the risks that CASPs are confronted with, and would mean that Union legislation is wanting in comparison to international standards. As a consequence, Member States would take steps to introduce AML/CT requirements for these operators individually, leading to diverging rules that would also make it difficult for CASP to operate across borders. As such, this option is considered sub-optimal.

The scope of entities subject to AML/CFT requirements is being aligned with the socope of entities subject to the requirements of the MICA regulation, which will ensure clarity on the side of the sector of the regulatory requirements they will need to comply with.

9. **Beneficial ownership**

[88] This rule requires that "countries should ensure that originating virtual assets services providers (VASPs) obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to the beneficiary VASP or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should also ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers and make it available on request to appropriate authorities."
[89] Regulation 2015/847 provides that "personal data shall be processed by payment service providers on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes".

As explained in the impact assessment, the lack of detail in relation to the application of the definition of beneficial ownership in practical cases has resulted in diverging methods across Member States to implement the same concept and definition. To address this, whilst leaving the current rules provisions unaltered, the preferred option is to clarify the current rules so as to achieve a consistent interpretation of the definition across the internal market.

The alternative, described in the problem definition, would be to leave it to Member States to determine how to identify beneficial owners. This approach leads to divergent outcomes that are inconsistent with the Union's ambition to achieve a high degree of transparency of beneficial ownership.

10. **FIUs**

The impact assessment has shown that important divergences exist still today in terms of the powers and functions of the FIUs across Member States. While the ability of FIUs to perform their tasks should be granted irrespective of their administrative set-up, there is evidence that today this has an impact on the amount of information that can be accessed by FIUs. Similarly, the core functions of FIUs are only presented in a general manner in the AMLD. As a consequence, the current framework does not draw a clear link between the core functions of FIUs and the powers that should be granted to them in order to perform such functions.

Moreover, as indicated in the impact assessment, the lack of clarity in EU rules as regards conditions and time limits for feedback to reporting entities, for requests for information as well as for suspension of transactions (or even bank accounts) has led to significant variations in the national rules that apply to the performance of these tasks.

To remedy this, the preferred option would:

- include a minimum set of common rules on the functions and powers of FIUs;
- maximum time-limits for requests of information or freezing of transactions/bank accounts.
- Clarify obligations for FIUs to provide feedback to entities/authorities reporting suspicions or cash declarations, and the circumstances when this should take place or exceptions to do so.

Since full harmonisation would fail to take account of the national specificities and instutitional frameworks, it seems appropriate to introduce the above measures whilst leaving Member States some margin on how to achieve them.

The alternative would be to let Member States introduce those provisions at national level. This is already the case but, as explained in the problem description, it has resulted in inefficient outcomes, with diverging powers and rights to access information necessary to perform financial analyses. This undermines the ability of FIUs to cooperate with one another and analyse cases of a cross-border nature.

11. **Supervision of non-financial sector entities**

The AMLD allows Member States to give to self-regulatory bodies (e.g. bar associations) the task of supervising entities in the non-financial sector. This option has been often resorted to by Member States, particularly when AML/CFT requirements apply to legal professions. However, as described in the problem definition, the quality and intensity of supervision applied by these self-regulatory bodies has been unsatisfactory.

Moreover, FATF recommendations provide that when supervision is performed by self-regulatory bodies, these should be supervised by a competent public authority in relation to such functions. Yet, the AMLD and most national legislation transposing it have failed to introduce this oversight obligation over the performance of self-regulatory bodies. As a result, under the current circumstances there is no effective framework in place to ensure that supervision in the non-financial sector is of adequate quality.

To address this, the preferred option is to include in the EU framework the FATF recommendation and ensure that there is actual public oversight over the supervisory practices of self-regulatory bodies. As not all Member States allow self-regulatory bodies to perform supervisory functions, it seems more appropriate to introduce public oversight whilst leaving Member States some margin on how to achieve it (i.e. through supervision of non-financial sector entities by a public authority or by a self-regulatory body overseen by a public authority).

The alternative option, i.e. to leave Member States free to decide whether to oversee the activities of self-regulatory bodies, would consist of the *status quo*. Its shortcomings have been presented in the problem description and would only be exacerbated in the context of stronger defences in the financial sector and a transfer of risks to the non-financial sector.

Given the need to ensure an adequate balance between the harmonisation of requirements that apply to obliged entities and the flexibility for Member States to devise national AML/CFT mechanisms, the different areas covered by the package of legislative proposals are so allocated to the different acts:

- Regulation: requirements that apply to obliged entities, legal entities and arrangements and private sector operators (e.g. list of obliged entities, internal policies, controls and procedures, CDD, BO information, reporting obligations, measures addressing bearer instruments);
- Directive: requirements that pertain to competent authorities (FIUs, supervision), cooperation among authorities; registers.

ANNEX 7: INTERCONNECTION OF BANK ACCOUNT REGISTERS

1. **Background and policy context**

The Commission has since 2016 underlined[90] the importance of the establishment of national centralised bank and payment account registers and central data retrieval systems, as such registers would provide direct operational support to the Financial Intelligence Units (FIUs) and would allow the consultation of these registers for other investigations (e.g. law enforcement investigations, including asset recovery, tax offences) and by other authorities (e.g. tax authorities, Asset Recovery Offices, other law enforcement bodies, Anti-corruption authorities).

Article 32(a) of the Fifth Anti-money Laundering Directive requires the Member States to put in place by 10 September 2020 national centralised automated mechanisms, such as central registries or central electronic data retrieval systems which allow the timely identification of any natural or legal person holding or controlling payment accounts, bank accounts or safe deposit boxes. Article 32(a)(3) defines the minimum set of data that should be made accessible and searchable through these mechanisms whilst Article 32(a)(2) provides the national FIUs with immediate and unfiltered access to this data and highlights that other competent authorities should also have access in order to fulfil their tasks and obligations under the Anti-money Laundering Directive.

More recently, Directive 2019/1153 on the use of financial and other information to combat serious crimes[91] extends the scope of authorities, able to access and search the national centralised automated mechanisms. The Directive obliges Member States to designate the national authorities competent for the prevention, detection, investigation or prosecution of criminal offences that should be empowered to access and search directly the minimum set of information contained in the national bank account registries and data retrieval systems. Those competent authorities shall include at least the Asset Recovery Offices (AROs), established by Council Decision 2007/845/JHA[92]. Member States may also designate tax authorities and anti-corruption agencies as competent authorities to the extent that these are competent for the prevention, detection, investigation or prosecution of criminal offences under national law. The Directive also sets out that access to and searches of the national bank account registries shall be performed on a case- by-case basis only by specifically designated and authorised staff in each competent authority that have been specifically designated and authorised to

[90] COM(2016) 50 final

[91] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, OJ L186 of 11.7.2019, pp. 122-137.

[92] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L 332, 18.12.2007, p. 103–105

perform those tasks.[93] The deadline for transposing the Directive is 1 August 2021.[94] Article 3(3) of Directive 2019/1153 requires Member States to notify the Commission of the competent authorities designated to access and search the centralised automated mechanisms by 2 December 2021.

Article 32(a)(5) of the Fifth Anti-money Laundering Directive requires the Commission to assess the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of the centralised automated mechanisms. The Commission's assessment, adopted in July 2019, concluded that the interconnection of the national centralised bank account registers and data retrieval systems is technically feasible.[95]

2. **State-of-play with regard to the setting up of centralised bank account registries and electronic data retrieval systems in the EU Member States**

At present[96], the vast majority of Member States have either already established centralised bank account registers and electronic data retrieval systems or are in the process of doing so. The majority of Member States have put in place centralised bank account registries (AT, BE, BG, CZ, ES, FR, HR, IT, LV, LT, MT, NL, PT, RO, SI) whereas other Member States have established electronic data retrieval systems (DE, DK, EE, EL, FI, LU and SE). In CY, a centralised bank account register has been developed, tested and populated by the Central Bank of Cyprus. Several Member States are in the process of setting up their centralised mechanisms pursuant to Article 32a of the Fifth Anti-money Laundering Directive. These are HU, IE, PL and SK.

All Member States with an operational register/retrieval system have granted their FIU and competent anti-money laundering authorities with direct access. Furthermore, in many Member States, where centralised bank account registries or electronic data retrieval systems exist, not only FIUs but also law enforcement authorities, including the AROs, have already a direct access to the centralised bank account registries (BE, BG, FR, DE, EE, EL, IT, LV, LT, LU[97], NL, SI). With the ending of the transposition period of Directive 1153/2019 on 1 August 2021, all Member States should have provided direct access to authorities competent for the prevention, detection, investigation or prosecution of criminal offences, including AROs.

Table X. Law Enforcement Agencies and Asset Recovery Offices direct access to account information

MS	Central bank Account Registry	Data Retrieval System	Direct access LEA	Direct Access ARO
AT	Yes	--	No	No
BE	Yes	--	No	Yes

[93] Article 5 (1).
[94] Article 23.
[95] COM(2019) 372 final.
[96] The information is based on the replies by Member States, provided at the Expert group meeting on Money Laundering and Terrorist Financing (EGMLTF) which took place on 6 and 7 October 2020.
[97] Only limited to money laundering / terrorism financing.

BG	Yes	--	Yes	Yes
CY	Yes	--	No	No
CZ	Yes	--	No	No
DE	--	Yes	Yes	Yes
DK	--	Yes	No	No
EE	--	Yes	Yes	Yes
EL	--	Yes	Yes	Yes
ES	Yes	--	No	No
FI	--	Yes	No	No
FR	Yes	--	Yes	Yes
HR	Yes	--	No	No
HU	n/a*	--	n/a	n/a
IE	n/a*	--	No	No
IT	Yes	--	Yes	No
LT	Yes	--	Yes	Yes
LU	--	--	Yes	No
LV	Yes	--	Yes	Yes
MT	Yes	--	Yes	Yes
NL	Yes	--	Yes	Yes
PL	No	No	n/a**	n/a**
PT	Yes	--	No	No
RO	Yes	--	Yes	No
SK	n/a*	n/a	n/a	n/a
SI	Yes	--	Yes	No
SE	--	Yes	Yes	Yes

Source: targeted questionnaire on ARO/law enforcement access to bank account information, October 2020.

Eleven Member States indicated that AROs have access to the access to bank account information, one of them indirectly and ten directly (including one of them with approval from the prosecutor). In thirteen Member States one or more law enforcement authorities have access to centralised bank account registries or data retrieval systems, in one case only for money laundering and terrorism financing investigations and in two cases following the approval from a judge or a prosecutor.

Judges and prosecutors themselves have access to bank account information respectively in five and in nine Member States (in two of them prosecutors only have such access for money laundering/terrorism financing cases). Five other Member States have indicated that they have given access to other authorities such as tax authorities, customs or intelligence services.

3. What is/are the problems?

A considerable part of criminal activity, especially serious and organised crime, is committed with the aim of creating a profit. Criminal revenues in the nine main criminal markets in the EU amounted to EUR 139 billion in 2019[98], corresponding to 1% of the Union's Gross Domestic Product (GDP). Criminals and terrorists operate in different Member States and their assets, including bank accounts, are located across the EU. They are quick to adapt and make use of modern technology that allows them to transfer money between numerous bank accounts and between different currencies in a matter of hours. Technological developments, such as the so-called 'real-time payments'

[98] Illicit drugs, trafficking in human beings, smuggling of migrants, fraud (MTIC fraud, IPR infringements, food fraud), environmental crime (illicit waste and illicit wildlife), illicit firearms, illicit tobacco, cybercrime activities, organised property crime – Study on Mapping the risk of serious and organised crime infiltration in legitimate businesses, March 2021, DR0221244ENN, https://data.europa.eu/doi/10.2837/64101.

technology[99], have significantly expedited the process of transferring money from one bank account to another. Modern technology brings benefits to financial institutions, merchants, consumers and society but also creates opportunities for criminals to instantaneously move their illicitly gained proceeds to different bank accounts in various Member States.

As highlighted in the 2016 Mapping exercise and gap analysis on FIUs' powers and obstacles for obtaining and exchanging information, bank account information is important both for domestic analysis and for the development of further cooperation and joint analysis between the interested FIUs as regards the detection of potential cross-border money laundering/terrorism financing carried out through bank accounts and assets held in multiple jurisdictions.

In order to determine the banks in other EU Member States, in which a person involved in transactions/activities suspected of a link with money laundering or terrorist financing activities holds a bank or payment account, the FIU of Member State A has to submit a request to the FIU of Member State B and wait for a reply. However, as highlighted in the 2016 Mapping exercise and the 2019 Commission report assessing the framework for cooperation between FIUs[100], the timeliness of responses to requests for information is a critical area where 'FIU-to-FIU' cooperation needs improving. The findings of the 2019 Commission report, for example, illustrate that the vast majority of FIUs reply to requests within the one-month period recommended by the Egmont Group of Financial Intelligence Units. However, the 2016 mapping report stressed that the 'current delays in receiving information… from counterpart FIU may have an impact on the effectiveness of analytical activities and ensuing law enforcement actions'.[101]

Moreover, such delays could also affect negatively the cases where an FIU needs to determine swiftly in which other Member States a subject of a postponement order suspending transactions holds bank or payment accounts. By doing so, the FIU will be able to proceed immediately with a request to its FIU counterpart to withhold consent to transactions and ensure that the funds and/or assets do not dissipate whilst the FIU analyses the transaction, confirms the suspicion and disseminates swiftly the results to the competent authorities. This is confirmed by the reply of one FIU to the questionnaire on exchange of and access to bank account information.[102] It pointed out that due to the

[99] Real-time payment schemes enable an instantaneous money transfer between banks and banking systems. They offer an instant, 24/7, interbank electronic fund transfer service that can be initiated through one of many channels, for example, smart phones, tablets, digital wallets and the web. In such a scheme, a real-time payment request is initiated that enables an interbank account-to-account fund transfer. An example of such a scheme is the UK Faster Payment Scheme (FPS) launched in 2008. Initially FPS was launched with a transaction limit of £10,000, rising to £100,000 in 2010 to a further £250,000 in 2015.
[100] COM(2019) 371 final
[101] The EU FIUs' Platform's "Mapping exercise and Gap Analysis on FIUs' Power and Obstacles for obtaining and exchanging information", endorsed by FIUs of all Member States on 11 December 2016, page 154. [to underline that this is not a commission document - this citation was used in previous FIU reports]
[102] The questionnaire was submitted to the FIUs prior to the FIU Platform meeting that took place on 5 October 2020. Several FIUs submitted replies in writing.

inefficiency of the current system, there are many cases where illicit proceeds cannot be seized or frozen. Another FIU pointed out that whilst urgent requests could be replied to within a day, in the vast majority of cases it takes its counterparts from other Member States between 15 to 60 days to reply to a request for information.

With terrorists and criminals operating across borders and money launderers and organised crime groups increasingly hiding and reinvesting assets in Member States other than the one where the original criminal act was committed, authorities competent for the prevention, detection, investigation and prosecution of criminal offences and AROs face similar problems as the ones affecting FIUs. Information on financial activities can provide law enforcement with crucial leads about subjects of an investigation and judicial authorities with invaluable evidence to ascertain the criminal acts of a person subject to criminal proceedings.

Moreover, swift access to bank account information is essential to ensure effective freezing and confiscation of proceeds of criminal activities, which are among the most effective means of combatting crime. However, confiscation rates are low: currently only about 2% of these assets are frozen, and only about 1% of are confiscated.[103] In order to trace, freeze and ultimately confiscate criminal assets that are stored on bank accounts, law enforcement authorities and AROs need to act quickly not to allow proceeds of crime to disappear. The information on whether a subject of an investigation holds a bank or payment account or a safe deposit box in a Member State other than one carrying out the investigation is essential for the identification of the Member States to which then subsequently freezing and confiscation orders have to be sent in order to secure the assets.[104]

Currently, in order to obtain information on persons who hold bank accounts in another Member State, law enforcement authorities may channel requests for such information via FIUs and, when this is not the case, they may exchange the relevant information cross border on the basis of bilateral police cooperation agreements or judicial cooperation instruments. This includes exchanges on the basis of Framework Decision 2006/960 JHA[105] (also referred to as the "Swedish Initiative"). Some Member States might require a European Investigation Order (EIOs).[106] For the recognition or execution of an EIO a

[103] Report on Asset recovery and confiscation: ensuring that crime does not pay, COM(2020) 217 final.
[104] On the basis of Council Framework Decision 2003/757/JHA and 2006/783 JHA, as of 19 December 2020 on the basis of Regulation 2018/1805.
[105] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, page 89 (referred to as the "Swedish initiative"). This instrument sets out rules for the exchanges of criminal information and intelligence information between law enforcement authorities. It sets out rules for the exchanges of criminal information and intelligence information and ensures that procedures for cross-border data exchanges are not stricter than those applying to exchanges at national level. It provides for the following time limits for exchanges of information: eight hours if the request is urgent and the information is in their databases; one week if the request is not urgent and the information is in their databases and two weeks if the request is not urgent and the information is not available in their databases.
[106] Directive 2014/41/EU.

deadline of 30 days applies, meaning that this is a lengthy process, hampering speedy access to information on persons who hold bank accounts.

Since 19 December 2020, Regulation (EU) 2018/1805[107] on the mutual recognition of freezing and confiscation orders applies.. This Regulation establishes precise timelines for the recognition and execution of freezing orders. In case immediate freezing is necessary (i.e. because there are legitimate grounds to believe that the property will imminently be removed or destroyed), the executing authority has 48 hours to decide on the recognition of the freezing order. Once the the decision on the recognition has been taken, the executing authority has 48 hours to take the concrete measures for the execution of the order. For confiscation orders, there is a maximum timeframe of 45 days to take a decision on their recognition and execution (see in this context Articles 9 and 20 of the Regulation).When issuing certificates for the mutual recognition of freezing and confiscation orders, Member States may indicate the details of the bank account of the affected person. Therefore, knowing where in the EU a suspect holds a bank account is invaluable information for competent authorities to quickly identify to which other Member States they should request the freezing and confiscation of money stored in those accounts before it is moved somewhere else.

4. What are the available policy options?

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

The baseline consists of the current status quo, whereby FIUs, other anti-money laundering authorities and designated authorities competent for the prevention, detection, investigation or prosecution of criminal offences are empowered to directly access and search the national centralised bank account registries at the national level. The baseline scenario coincides with the first pillar of the Commission's Action Plan in relation to the effective application of the existing relevant rules, i.e. the EU Anti-money Laundering Directive and Directive 2019/1153. The Commission would monitor such transposition and would open infringement proceedings in case of incomplete or incorrect transposition.

However, authorities would not have any cross-border access to bank account information. In this respect, it is very likely that the problems described in section 3 would persist and would even exacerbate with time as technologies will continue to develop and evolve, thus, providing criminals with the opportunity to transfer money between various bank accounts within or outside the EU expeditiously.

In the case of FIUs, even the imposition of mandatory time limits for replies will not resolve the ongoing problems linked to the high workload of the FIUs, which would continue to have to deal with an increasing amount of such requests. Moreover, the requesting FIU will have to wait to receive a reply with the requested information by its

[107] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders

FIU counterpart. This will have an impact on the rapidity of the financial intelligence produced and its usefulness for law enforcement authorities.

As regards other competent authorities, the baseline would entail reliance on existing channels of communication for requests for information exchanges between the competent authorities based on their access to the national central registers. This would either result in (a) an increased workload for competent authorities to respond to cross-border requests from competent authorities in other Member States or (b) that competent authorities choose not to enrich their analysis/investigations with bank account information that is available in other Member States due to a slower and less efficient procedures. This would also reduce the amount of assets that are detected, identified, frozen and, ultimately, confiscated.

4.2. Description of the policy options

Two policy options could address the operational shortcomings and problems described in the previous two sections.

4.2.1. Provide FIUs with direct access to the platform interconnecting the national centralised bank account registries

The first policy option envisages providing FIUs with direct access to the platform interconnecting the national centralised bank account registries in order to fulfil their obligations under the Anti-money Laundering Directive.

This option provides for a more restrictive approach, whereby, for example, law enforcement authorities (including AROs) are not granted with access to the platform interconnecting the bank account registers for the purposes of fighting serious criminal offences. This would undoubtedly have a limited impact on effectiveness as the problems identified above would to a very large extent persist as regards law enforcement authorities and AROs still having to rely on the existing channels to access and exchange bank account information.

4.2.2. Provide FIUs and authorities competent for the prevention, detection, investigation or prosecution of criminal offences with direct access to the platform interconnection the national centralised bank account registries

This option builds upon option 1 and covers a broader range of authorities. Firstly, similar to option 1, it provides FIUs with direct access to the platform interconnecting the centralised bank account registries. Secondly, it also provides the competent authorities designated by the Member States pursuant to Article 3(1) of Directive 2019/1153 with the power to access and search directly the interconnection platform.

The Commission's report on the interconnection of centralised bank account registers of July 2019 concluded that such an interconnection would speed up access to financial information and facilitate the cross-border cooperation of the competent authorities. The

Action plan for a comprehensive Union policy on preventing money laundering and terrorist financing, adopted by the Commission in May 2020, emphasised that an 'EU-wide interconnection of central bank account mechanisms is necessary to speed up access by FIUs and law enforcement authorities to bank account information and facilitate cross-border cooperation' and that it should be considered as a matter of priority.[108] In this context, it is worth highlighting that the June 2020 Council conclusions on enhancing financial investigations to fight serious and organised crime called on the Member States to engage in a constructive discussion with the Commission regarding the future interconnection of national bank account registers and data retrieval systems. Moreover, the Council also called on the Commission to consider further enhancing the legal framework in order to interconnect the national registers and retrieval systems in order to accelerate access to financial information and facilitate cross-border cooperation between the competent authorities and their European counterparts.[109] The Security Union Strategy adopted in July 2020[110] also refers to the interconnection of national centralised bank account registries, which could significantly speed up access to the financial information for Financial Intelligence Units and competent authorities.

Finally, the European Parliament's resolution of 10 July welcomes the Commission's "plan to ensure interconnection of centralised payment and bank account mechanisms across the EU in order to facilitate faster access to financial information for law enforcement authorities and FIUs during different investigation phases and facilitate cross-border cooperation in full compliance with applicable data protection rules".[111]

These repeated calls for the centralised bank account registers to be interconnected and access to be granted to both FIUs and authorities competent for the prevention, detection, investigation or prosecution of criminal offences reflect the operational needs of those bodies and indicate that this is the preferred option that would be assessed in greater detail below, in particular, as regards its impacts on effectiveness, proportionality and costs.

5. What are the impacts of the preferred policy option?

5.1. Effectiveness of the preferred option

Swift access to and exchange of information on bank accounts is of fundamental importance for the successful fight against money laundering and terrorism financing and more generally for combatting serious crime. Direct cross-border access to bank account information would allow FIUs to produce financial analysis within a sufficiently short timeframe to detect potential money laundering and terrorism financing cases and guarantee a swift law enforcement action.

[108] COM(2020) 2800 final.
[109] 8927/20.
[110] COM (2020) 605 final.
[111] European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments (2020/2686(RSP)).

The effectiveness of the preferred option and its operational benefits are demonstrated by the practical examples, given below.

Practical example of potential operational benefits for FIUs (I)

FIU A is chasing illicit proceeds transferred through bank accounts in several Member States. The perpetrators are able to transfer the money through different foreign bank accounts. FIU A must request its counterpart FIUs in the respective Member States and wait for their replies in order to identify in which countries the person(s) under suspicion for links to money laundering or terrorist financing have bank accounts. A more efficient system would resolve the current challenged, faced by the FIUs and will lead to the more effective freezing and seizure of illicit assets.

The interconnection of bank account registers will significantly improve FIUs' capacity to obtain swiftly bank account information held in other EU Member States. Consequently, FIU-to-FIU requests will not be required to identify the banks in other Member States, in which a person involved in transactions/activities suspected of a link with money laundering or terrorism financing holds bank accounts. This will further optimise the cooperation between the national FIUs and strengthen their ability to produce rich financial analysis, which is essential for the prevention of money laundering and terrorist financing and for law enforcement to uncover criminal activities, trigger new investigations and contribute to ongoing ones.

The potential operational advantages of a system interconnecting the bank account registers was also confirmed by the replies of another FIU to the above-mentioned questionnaire. FIU B stressed that given the increasing number of exchanges of information per year[112], the direct access to bank account information held in other Member States will have a positive impact on the average response time when the requests concern this type of information. This will consequently provide the FIUs with more time to spend on other tasks related to the exchange of information or analysis.

Practical example of potential operational benefits for FIUs (II)

Requests received: A large number of requests for information submitted to FIU B are related to scams (e.g. phishing, business email compromise (BEC) fraud), where for fraudulent reasons funds are sent to a bank in Member State B. Many of the requests FIU B receives only concern the identity details of the bank account holder. Direct access by FIUs to the interconnection system will make this kind of requests unnecessary and will provide FIU B with more time to spend on other tasks.

Requests sent: A significant number of the requests FIU B sends abroad are related to police investigations and aim to identify potential bank accounts in other Member States, which are somehow linked to the investigation and the 'person of interest'. However,

[112] The latest statistics on the use of FIU.net for the period of 1 January 2020 – 31 August 2020 show there were 13,190 outgoing requests, which represents an increase of 13.5% compared to the same period last year.

they only request information from countries which are linked to the investigation. A system interconnecting the bank accounts may reveal existing bank accounts in countries without an obvious link to the investigation.

The interconnection of bank account registers will also significantly improve the effectiveness of the investigations carried out by authorities competent for the prevention, detection, investigation or prosecution of criminal offences and further strengthen the abilities of the national AROs to trace and identify proceeds of crime by facilitating cross border cooperation and speeding up access to information on whether a person object of a criminal investigation or judicial proceeding holds a bank account in another Member State. This information is essential for the above-mentioned authorities and AROs to swiftly identify the Member States to which they should send, respectively, requests for further information (for investigative or evidential purposes) or freezing and confiscation orders to secure the assets.[113]

The interconnection of bank account registers will significantly improve the capacity of authorities competent for the prevention, detection, investigation or prosecution of criminal offences to obtain swiftly information on where a suspect in a criminal investigation into serious crimes holds bank accounts in other EU Member States. It will be an important element to enhance freezing and confiscation of criminal assets and step up confiscation rates.

Practical example of potential operational benefits for law enforcement authorities

Law enforcement authorities in Member States A and B receive a request of the law enforcement authority in Member State C in a criminal investigation in a big drug trafficking case to identify bank accounts held by the suspect. Law enforcement authorities in Member States A and B have a direct access to their national bank account registries. Member State A answer within a few hours, whilst Member State B provides the information after 1 week. When the law enforcement authority or the ARO in Member State C, on the basis of this information, requests freezing orders at the competent court, and subsequently issues European Investigation Orders/certificates for the mutual recognition of freezing orders in order to freeze the substantial sums of money in the accounts, most of it has already disappeared.

A system interconnecting the bank accounts would speed up the tracing and identification of proceeds of crime in cross-border scenarios in view of their possible freezing and confiscation, as it would allow the identification of the banks where a suspect holds bank accounts within a very short period of time.

5.2. **Proportionality of the preferred option**

[113] On the basis of Council Framework Decision 2003/757/JHA and 2006/783 JHA, as of 19 December 2020 on the basis of Regulation 2018/1805.

The proposed measure is proportionate to the objective to further strengthen the national authorities' ability to fight money laundering, its associated predicate offences and the financing of terrorism and, more generally, serious crime. Solely specifically designated authorities will be provided with direct access to bank account information through this interconnection. These will include the FIUs[114], other competent national authorities in order to fulfil their obligations under the Anti-money Laundering Directive as well as the competent authorities and AROs, designated pursuant to Article 3(1) of Directive 2019/1153 to access and search its national centralised bank account registry.

Whilst under the Anti-Money Laundering Directive, the purpose of the centralised mechanisms on bank accounts is to improve the fight against money laundering and terrorist financing and access is limited to certain public authorities, the Directive on facilitating access to financial and other information extends the purpose of the use of the information in the central mechanisms to serious crime and the access rights to designated competent authorities. Finally, the specific domestic authorities having direct access to the national registries lies with the Member States operating the registries, but the Directive requires that these are "authorities competent for the prevention, detection, investigation or prosecution of criminal offences" and that they should at least include the AROs. Therefore, as set out in 2019 report on the interconnection of national centralised bank accounts registries,[115] the same authorities, which will be provided with direct access to the centralised mechanisms in accordance with the Anti-Money Laundering Directive and the Directive on facilitating access to financial and other information, will be provided with access to the interconnection platform.

For the authorities granted access under the national laws to also access and search the EU-wide interconnection system, detailed provisions on the conditions for access and searches by the competent national authorities would be necessary. In this regard, it is important to highlight that the Directive on the use of financial information and other information lays down strict conditions for the access and for searches of bank account information contained in the centralised automated mechanisms by competent authorities designated at national level[116]. Such conditions include, for example, the provision of access to the registries and data retrieval systems only to specifically designated and authorised persons of each competent authority. Another safeguard is the restriction of the scope of the available information in the interconnection system to the minimum set of information relating to the account profile as set out in Article 32a(3) of the Anti-Money Laundering Directive.

[114] It is important to highlight that the EU FIUs can be grouped under three models as regards their institutional nature and organisation: administrative, law enforcement (or judicial) and 'hybrid'. The nature and institutional setting of the FIUs can have an impact on their analytical functions of suspicious money laundering and terrorist financing cases.
[115] COM (2019) 372 final.
[116] Directive (EU) 2019/1153. This Directive is based on article 87(2) of the Treaty, and therefore any opening of interconnected bank account registries to authorities competent for the prevention, detection, investigation or prosecution of criminal offences would normally have to use the same Treaty base.

In accordance with the principle of 'data minimisation', the interconnection will only concern specific sets of data which enable the querying authority to determine in which banks and Member States a 'person of interest', suspected of links to money laundering or the financing of terrorism, holds a bank or payment account or a safe deposit box. The following limited set of information will be accessible and searchable through the EU interconnection platform:

- for the customer-account holder and any person purporting to act on behalf of the customer: the name, complemented by either the other identification data required under the national provisions transposing point (a) of Article 13(1) of the Fifth Anti-money Laundering Directive or a unique identification number;
- for the beneficial owner of the customer-account holder: the name, complemented by either the other identification data required under the national provisions transposing point (b) of Article 13(1) of the Fifth Anti-money Laundering Directive or a unique identification number;
- for the bank or payment account: the International Bank Account Number (IBAN) number and the date of account opening and closing;
- for the safe-deposit box: name of the lessee complemented by either the other identification data required under the national provisions transposing Article 13(1) of the Fifth Anti-money Laundering Directive or a unique identification number and the duration of the lease period.

Therefore, the access to and search of sensitive data, such as information on transactions or balance of bank accounts will not be possible. Only information, strictly necessary to identify a holder of a bank or payment account or a safe deposit box, will be made accessible through the interconnection system.

Moreover, the applicable safeguards will ensure the respect for and protection of individual rights, such as the right to the protection of personal data and the right to private life. In line with Opinion 5/2020 of the European Data Protection Supervisor[117], the interconnection works will embed the principles of data protection by design and data protection by default in accordance with Article 25 of Regulation (EU) 2016/679.[118] Furthermore, strong data protection safeguards will be established, particularly concerning access rights and the accuracy of data pursuant to Article 5(1)(d) of Regulation (EU) 2016/679. The details of every access to the interconnection platform will be recorded in a log which will be stored for at least a defined period of time. These access logs will be subject to regular checks by data controllers and data protection supervisors. The access to and searches of information through the interconnection system will be carried out only on a case-by-case basis only by staff of the respective

[117] European Data Protection Supervisor, Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing, available at: https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_en.pdf.
[118] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

authority that have been specifically designated and trained to carry out those tasks. Finally, procedures pertaining to the authorisation/approval of access to bank account information held in a Member State other than the one of the requesting authority will be considered.

5.3. **Costs of the preferred option**

The interconnection of the centralised bank account registries and electronic data retrieval systems will generate costs both in terms of establishing the system and its maintenance. In its July 2019 report on the interconnection of bank account registers, the Commission considered several model examples of existing EU systems and the costs linked to their establishment in order to provide an indicative figure of the potential expenses that the interconnection of bank account registers will entail. In the majority of examples considered, the costs linked to the EU component interconnecting the various national databases (the EU platform or central routing component) were covered by the EU budget, whereas the Member States bore the costs linked to the modification of their national systems in order to make them interoperable with the EU central component.

For example, the costs for the development of the first version of the Business Register Interconnection System (BRIS) amounted to approximately EUR 1,700,000. As regards the insolvency registers interconnection system (IRI), the setting up of the central search pilot system (IRI 1.0) cost approximately EUR 280,000, whereas its adaptation towards the establishment of IRI 2.0 is estimated to amount to approximately EUR 170,000. Furthermore, with regard to the European Criminal Records Information System (ECRIS) the costs of the development of the software to exchange criminal records data between the Member States reached EUR 2,050,000, whereas its annual maintenance amounts to approximately EUR 150,000.

Finally, in order to assess the costs for the establishment of a direct connection to a system, the connection costs of the AROs to the Europol SIENA system or the costs incurred by Business Registers Interconnection System (BRIS) project to set up the network between relevant authorities can be used as proxies. The basic cost of these connections varies between EUR 5 000 and EUR 30 000 per authority. These costs have then to be multiplied by the number of authorities connected to the network.[119]

Thus, the costs linked to the interconnection of the bank account registers and the provision of access to FIUs, other anti-money laundering authorities and law enforcement authorities appear rather low compared to the benefits such a project would bring in the fight against money laundering, associated predicate offences and the financing of terrorism.

[119] This information was provided in the context of the impact assessment accompanying Proposal for a Directive of the European Parliament and of the Council on laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences and repealing Council Decision 2000/642/JHA, SWD(2018) 114 final

ANNEX 8: EU POLICY TOWARDS THIRD COUNTRIES WITH STRATEGIC DEFICIENCIES IN THEIR AML/CFT REGIMES

1. Background and policy context

The policy towards third countries is established under Article 9 of the AMLD that empowers the Commission to adopt delegated acts in order to identify high-risk third countries (HRTCs), taking into account strategic deficiencies, and laying down the criteria on which the Commission's assessment is to be based. The delegated acts have to be adopted within one month after the identification of the strategic deficiencies. Based on this identification, obliged entities are required by Article 18a of the AMLD to apply Enhanced Due Diligence (EDD) measures when establishing business relationships or carrying out transactions involving HRTCs identified by the Commission. In addition, Article 155(2) of the Financial Regulation institutes a ban on entering into new or renewed operations with entities incorporated or established in high-risk third countries, unless the action is physically implemented in such jurisdictions.

The Commission adopted the first Delegated Regulation in 2016[120], identifying as "high-risk" third countries previously listed by the Financial Action Task Force (FATF). The FATF is the global standard setter on combatting money laundering and the financing of terrorism, in which the European Commission along with 14 Member States are founding members, actively involved in the assessment by the FATF of countries possibly presenting strategic deficiencies. Subsequent amendments of this Delegated Regulation were rejected by the European Parliament, which called on the Commission to fulfil its obligation based on an autonomous assessment rather than solely replicating lists adopted by FATF[121]. Consequently, the Commission made a commitment to develop a methodology for identifying HRTCs. A methodology was set out in a Commission Staff Working Document published on 22 June 2018[122].

On 13 February 2019, the Commission adopted a Delegated Regulation on HRTCs pursuant to Article 9 of the AMLD and applying such a methodology. This Delegated Regulation was rejected by the Council on procedural grounds, as "not established in a transparent and resilient process that actively incentivises affected countries to take decisive action while also respecting their right to be heard"[123]. In its resolution of 14 March 2019[124], the European Parliament regretted the rejection by the Council, welcomed the Commission's methodology, and recalled that an EU delegated act is a separate process from the FATF listing and should remain exclusively an EU matter.

---

[120] Delegated Regulation (EU) 2016/1675

[121] See Resolution P8_TA(2017)0008, Resolution P8_TA- (2017)0213 and the Report on the inquiry into money laundering, tax avoidance and tax evasion (2017/2013(INI))

[122] SWD(2018) 362 final available at; https://ec.europa.eu/info/sites/info/files/swd_2018_362_f1_staff_working_paper_en_v2_p1_984066.pdf

[123] https://data.consilium.europa.eu/doc/document/ST-6964-2019-REV-1/en/pdf

[124] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2019-0216&format=XML&language=EN

Following this, on 7 May 2020 the Commission published a refined Methodology for identifying high-risk third countries[125], which addresses the interaction between the EU and FATF listing process, provides for an increased synergy with the FATF listing process, an enhanced engagement with third countries and a reinforced consultation of Member States' experts.

The refined Methodology lays down two main ways, which could lead to a country's identification as a "high-risk": (i) countries publicly identified by the FATF and (ii) countries assessed autonomously by the EU.

Firstly, any third country listed by the FATF will be in principle listed by the EU. Considering the high level of integration of the international financial system, any third country representing a risk to the international financial system, as identified by the FATF, is presumed to represent a risk to the internal market and is consequently listed by the EU. For the countries included in the EU scope, the Commission assesses whether the FATF action plans are sufficiently comprehensive, also in view of the EU delisting criteria and the specific EU requirements, in particular on ensuring transparency of beneficial ownership information. Only when this is not the case, further mitigating measures ("EU Benchmarks") would be developed to "top-up" the existing FATF Action Plan. The Commission ensures appropriate engagement with third countries in that case.

The FATF lists constitute the baseline for the EU list and this methodology builds on the listing process followed by FATF. At the same time, as the threats to the financial system of the Union are more specifically defined than those to the global financial system, the Commission should also conduct an autonomous assessment of third countries' AML/CFT regime. The Commission services focus on:

a. Countries identified by the Commission services, the EEAS or Europol as having a systemic impact on the integrity of the EU financial system due to the level of threat.
b. Countries identified as international offshore financial centres.
c. Countries with an economic relevance for the EU (considering the magnitude of the financial centres and the strength of economic ties with the EU).

The Commission services identify priorities and carry out an autonomous assessment. The Commission engages with third countries at an early stage.

The EU list was aligned with the FATF through the Delegated Act adopted on 7 May 2020, along with the publication of the revised methodology.

2. Challenges of the current policy

The aim of the EU policy towards high-risk third countries is to protect the financial system of the Union and the proper functioning of the internal market. The consequences of a EU listing is mandatory EDD applied by obliged entities in the EU in relation to all

[125] SWD(2020) 99 final available at https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology_en.pdf

operations with the concerned third country and counter-measures by Member States to be adopted from a menu foreseen in the AMLD.

The current approach does not always allow for the needed dynamism and flexibility to respond to evolving external AML/CFT risks. It has revealed a number of limitations:

- The current EU approach does not differentiate between countries which are committed to address their shortcomings (FATF grey list) and those which are non-cooperative (FATF black list).
- There is currently a fragmented approach within the internal market, as the determination of which EDD measures to apply among those listed under Article 18a of the AMLD is currently entirely left to the decision of the Member States.
- It is extremely difficult to impose enhanced vigilance requirements for a country which is not on a FATF list. The only available measure under the current process to apply enhanced vigilance would be through an autonomous listing. This may hinder effectiveness.
- The restrictions under the EU Financial Regulation with regard to cooperative countries (FATF grey list) might be also considered disproportionate by some stakeholders.

Another challenge is the question of the publication of the countries which made a high level political commitment and of the assessments of third countries. The European Parliament calls on the Commission to have a grey list so that third countries having made high level commitments to change their standards and comply with the EU benchmarks are known to the public. Addressing this demand is challenging for several reasons. Publishing a "grey list" based on preliminary assessments could expose the Commission to legal risks and impair an ongoing decision-making process. It could also undermine the protection of the public interest regarding international relations and the financial, monetary and economic policy given the possible impact on financial markets.

The main challenge encountered in the Commission's efforts to implement this policy lies in the different interests held by key stakeholders: on the one hand, for an increasingly ambitious and all-encompassing policy, favoring a list of third countries autonomously identified by the EU, on the other hand for not departing from the well-established FATF listing process.

3. Possible options for a future policy

The future policy should take into account several objectives. Compliance with international standards, notably FATF Recommendation 19 on higher-risk countries, must be ensured. An appropriate balance needs to be found between, on the one hand, the need to preserve an ambitious policy towards third countries and, on the other hand, the need to implement a more consistent approach while ensuring enhanced effectiveness in protecting the internal market from external threats.

Three broad options exist: the status quo (baseline scenario); an option of abandoning any kind of formal EU listing system (leaving it entirely to Obliged Entities to determine

the specific measures to adopt regarding high risk third countries), and an intermediate option providing a greater degree of harmonization of countermeasures/EDD and allowing for input and guidance from the new AML Authority. This intermediate option, described in more detail below, could consist of **a mechanism based on three pillars**: (i) countermeasures; (ii) enhanced due diligence; and (iii) advice on risks and trends. Such a mechanism could have the following features:

(i) Countermeasures

The Commission should be empowered to adopt implementing regulations identifying third countries subject to an FATF call for action ("blacklisted countries"), which would set out countermeasures applicable to all EU obliged entities, based on the FATF calls.

This would allow for a uniform approach at Union level that would reduce fragmentation in the regulatory landscape and remove weak links in the internal market. It would ensure **uniform conditions for implementing countermeasures within the internal market**. Obliged entities will have common rules within the internal market. Furthermore, the credibility of the EU acting as a single jurisdiction to address ML/TF risks would be strengthened.

(ii) Adoption of enhanced due diligence measures following a grey listing by FATF or independently

The EU framework must be able to require financial institutions to apply EDD measures that are proportionate to the risks, as regards third countries which **the FATF has listed (both blacklisted and greylisted)**.

At the same time, the EU should maintain a mechanism to require the application of specific and binding EDD **requirements independently from FATF** to address risks posed by third countries. The Commission would be empowered to adopt delegated regulations, which would set the common EDD that Member States must take, based on the risks identified at EU level. Member States would be able to apply supplementary EDD, based on the specific risks identified at national level.

EDD measures at Union level could concern in part countries grey-listed by the FATF, based on risks they pose to the EU, but also countries which are not identified by the FATF listing process.

Compared to the baseline scenario, there would be a greater degree of harmonization of EDD measures for those third countries which are listed by the Commission, either following their greylisting by FATF or independently. At the same time, that approach would be granular and commensurate with the level of threat identified for each third country.

The EU AML Agency would provide input to the Commission on the identification of EDD.

(iii) Provision of advice regarding concerns about weaknesses, risks and trends

Obliged entities throughout the Union would be advised of concerns about weaknesses, risks and trends, in accordance with FATF Recommendation 19[126]. This would replicate the current practice at Member State level, where regulators or supervisors inform obliged entities about weaknesses in third countries' AML/CFT regimes, by sharing the FATF public statement and FATF compliance documents. This could be accompanied by an advice for taking appropriate risk-based measures. Financial Intelligence Units (FIUs) would provide reports on risk typologies, methods and trends – advising obliged entities to apply enhanced vigilance based on identified *modi operandi* / risk-scenarios.

A replication at Union level of good yet fragmented practices at national level could be addressed by the **EU AML Authority**. The EU AML Authority could provide **advisory guidance on third country risks**. This guidance would complement, easily and effectively, the binding EDD measures under the second pillar by issuing softer measures.

The **EU AML Authority** could also provide **guidance** to obliged entities on concerns about **weaknesses in the AML/CFT systems of third countries**. It would at least disseminate FATF public statements and FATF compliance documents after each FATF meeting. It could also produce further information on third countries' deficiencies in their AML/CFT regime (like the US International Narcotics Control Strategy Reports).

The **EU AML Authority** could provide **guidance on risk typologies, methods and trends.** It could issue such advisory guidance on a "transactions-based approach" and recommend enhanced vigilance based on specific *modi operandi*/risk scenarios (i.e. non-mandatory EDD measures based on risks, trends and context).

Such a mechanism relying on the 3 pillars described in i)-iii) above would rely on the support of the future EU AML Authority, while all decisions would remain a prerogative of the Commission. These would be adopted by means of Implementing or Delegated Regulations.

The revised policy towards third countries would ensure an efficient process that **minimises risks for the EU,** while ensuring that the divergent interests of stakeholders are duly accounted for. It will also provide for an effective and efficient process to **manage risks posed by third countries**, allowing timely adoption of specific measures proportionate to the risks that such countries pose to the stability of the EU financial system. Finally, it would ensure **compliance with international standards**, notably FATF Recommendation 19 on higher-risk countries.

[126] C.19.3 provides that countries should have measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries.

ANNEX 9: INTRODUCTION OF CASH LIMITS

1. **Background and policy context**

Recital 6 of the AMLD recognises that the use of large cash payments is highly vulnerable to money laundering and terrorist financing. In order to increase vigilance and mitigate the risks posed by such cash payments, the Directive subjects persons trading in goods to AML/CFT requirements when they make or receive cash payments of 10 000 EUR or more, including through linked payments. This measure does not amount to a blanket restriction on the use of cash, and its effectiveness heavily hinges on faithful adherence and implementation by private sector as well as effective oversight on part of national public authorities Therefore, the Directive recognises that Member States may take different approaches, and allows them to lower the above threshold, introduce additional general limitations to the use of cash, or adopt other stricter measures.

In its Report to the European Parliament and the Council on restrictions on payments in cash of 12 June 2018[127], the Commission noted that introducing cash limits at EU level could have potential benefits on fighting money laundering. The report also concluded that diverging national provisions on payments in cash distort competition in the internal market, leading to potential relocations of businesses across borders, in particular for some specific sectors relying significantly on cash transactions, such as jewellery or car dealers. The report finally noted that diverging national restrictions potentially create loopholes allowing the bypassing of national cash payment limits, therefore decreasing their efficiency.

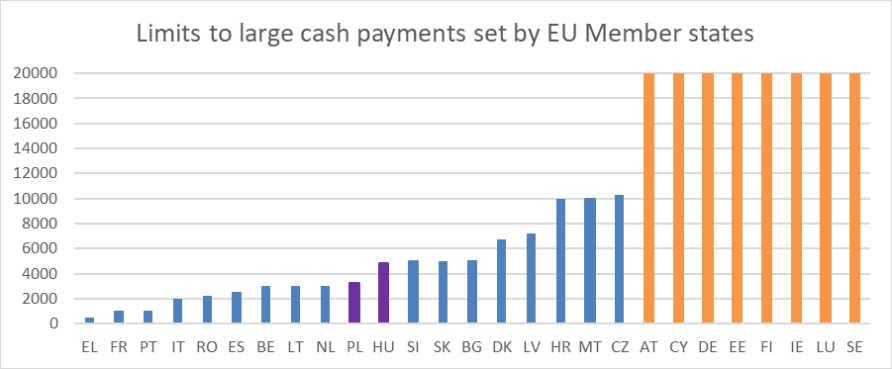
The Action plan for a comprehensive Union policy on preventing money laundering and terrorist financing, adopted by the Commission in May 2020, noted the different approaches taken by Member States to mitigate the ML/TF risks associated with cash. The Action Plan pointed out that the introduction of ceilings for large cash payments is one of the measures that could deliver a reinforced AML/CFT rulebook.

In reaction to the Action Plan, the Council conclusions of 17 June 2020 on enhancing financial investigations to fight serious and organised crime noted that the analytical work done by the Commission and Europol shows that criminals use cash payments to launder money and to finance terrorism. The conclusions called on the Commission to re-engage in a discussion with Member States on the need for a legislative limitation on cash payments at EU level.

[127] COM(2018)483 final

2. **State-of-play with regard to the setting of cash ceilings across the European Union**

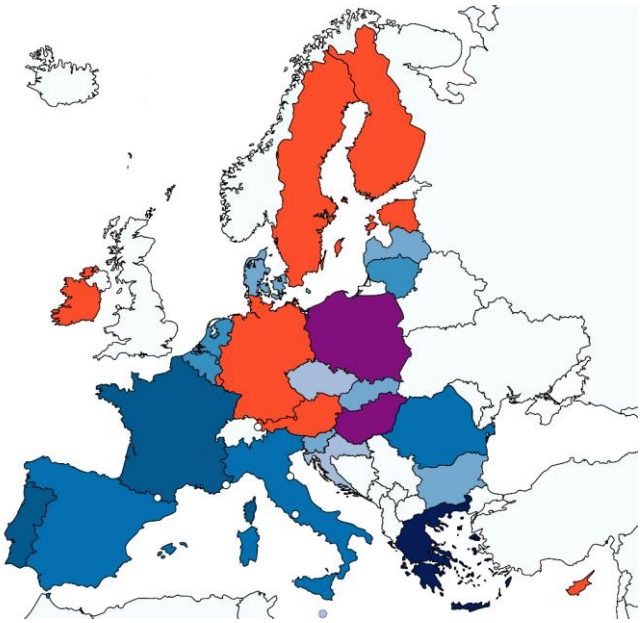
Currently, 19 Member States have introduced or are introducing limitations to cash payments128, ranging from EUR 500 in Greece to EUR 10 300 in Czechia, with an average value of about EUR 4 500129. The situation is constantly evolving, with Malta having recently introduced a limit of EUR 10 000 to payments in cash for some sectors, and other Member States having decided or planning to lower these limits (e.g. Denmark is planning to lower the limit to DKK 20 000 / EUR 2 700 and Italy will see its limit lowered to EUR 1 000 as of 2022). In three cases (France, Italy and Spain), higher thresholds apply to non-residents (between EUR 10 000 and EUR 15 000), and while in Hungary and Poland limits apply only to B2B transactions, some countries such as Slovenia have set different thresholds for B2C and B2B transactions. Among the countries that have not set any limit to cash payments, Ireland and Sweden allow traders to refuse payments in cash. The graph below summarises the situation across EU Member States.



Orange: no cash limits set – HU, PL: limits only apply to business-to-business transactions

The map below provides a graphical representation of the intensity of the cash limits set (from the darkest to the lightest blue), where they exist, and where countries without cash limits are located. The map shows that generally neighbouring EU countries have applied different thresholds or often taken different approaches (limit/no limit), which impacts on the effectiveness of the national measures and on the level playing field across the internal market as the next section will show.

[128] In the case of the Netherlands, this is a draft proposal approved by the government on 25 September 2020.
[129] Figures refer to B2C transactions.



3. **The impacts of the absence of a common limit to cash transactions at EU level**

AML/CFT experts and practitioners, from academics to law enforcement authorities, are unanimous that while cash is slowly falling out of favour with consumers, it remains the criminals' instrument of choice to facilitate money laundering.[130] This was reflected in the 2019 SNRA, following a large consultation of Member States and taking into account their national risk assessments, which noted the "very significant" exposure to ML/TF threat of cash payments, and that the variety of regulations on cash payments among Member States increases the vulnerability of the internal market.

Despite the changing face of criminality, with significant threats now stemming from new technologies, such as online frauds and illicit online marketplaces, money laundering methods remain overwhelmingly traditional and cash is still one of the most prevalent facilitators for money laundering across almost all criminal activities.

The risks associated to cash are reflected in the fact that the use of cash is still the main reason triggering reports of suspicious transactions within the financial system. However,

[130] FATF REPORT *Money laundering through the physical transportation of cash*, October 2015: http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf.
Europol, *Why is cash still King? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*, 2015: https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering
ECORYS, *Study on an EU initiative for a restriction on payments in cash, Final Report*, 2017: https://ec.europa.eu/info/sites/info/files/economyfinance/final_report_study_on_an_eu_initative_ecorys_180206.pdf

when it comes to prosecution, it is challenging to demonstrate the link between cash and criminal activities.[131] This is because most EU legal framework still impose demonstrating the predicate offence in order to prosecute money laundering, and given that cash is a bearer instrument, this is a challenging task.

Example: Cash generated by criminal activities laundered by the purchase of high value goods and properties (Europol Report "*Why is cash still king*")

Money from the sale of drugs was collected in Member State 1 and its laundering was orchestrated through the movement of cash by couriers acting as mules from Member States 1 to Member States 2, where cash was used to buy gold. Thereafter, gold was transported to and made into jewellery in a third country. A key organiser admitted laundering EUR 36 million since 2010 and sending 200 kg of gold from EU to the third country. The network collected about EUR 170 million per year.

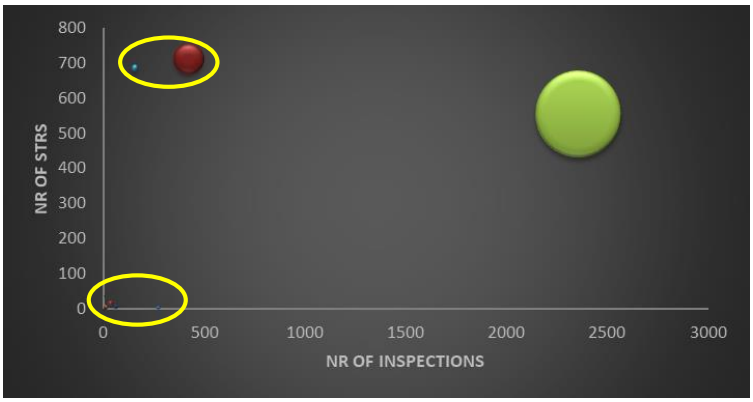
A cash payment threshold in Member State 2 would have reduced the profitability of this criminal scheme (as intermediaries have to be paid and multiplying transactions to change cash into gold by non-professional would have aroused more suspicion).

High value goods (such as watches, art works, luxury vehicles, precious metals and jewels) or real estate offer criminals an easy way to integrate funds into the legal economy, converting criminal cash into another class of asset which retains its value and may even hold opportunities for capital growth. In addition, these items can be moved across borders undetected and thereafter sold, as they are not captured by the existing rules on cash control and need not be declared.

Impacts on effectiveness

In the absence of a common limit to cash transactions, the current AML/CFT system relies, as explained above, on the obligation for traders in goods to apply AML/CFT rules to transactions amounting to EUR 10 000 or more. However, the effectiveness of those measures is very limited. The volume of suspicious transactions reported by these sectors is generally low, with one notable exception where hundreds of suspicions have been reported by these sectors. However, even in this case the intensity of reporting is very low (less than 0,1% of traders in goods reported one suspicion). This is because cash transactions are difficult to detect, there are few available information and traders applying AML/CFT rules may lose their clients to the benefit of competitors applying looser controls. Even when currency transactions are reported (e.g. upon withdrawal of large sums of cash), the lack of suspicions linked to these transactions does not allow FIUs to produce financial intelligence of significance. In addition, it may be difficult for a trader in high value goods to design an AML/CFT policy in the limited events where a cash transaction beyond the threshold takes place. This is linked to very limited supervision across Member States over a very wide set of operators, as the chart below shows.

[131] To facilitate prosecution, France has for example introduced provisions that allow reversing the burden of proof (i.e. when transfer of cash above EUR 10.000 are detected, their legal origin must be proven).



Size of the bubble reflects the size of the sector (variation: between 100 and 800.000).

For this reason, several Member States have extended the scope to cover certain sectors regardless of the use of cash or introduced a general cash restriction regime. However, as noted above, diverging national restrictions weaken the effectiveness of national cash threshold, by displacing illegal activities from a Member State with cash payment restrictions to a neighbour with more lenient restrictions or no restrictions at all. This was confirmed by anti-mafia Prosecutor Nicola Gratteri at the Commission's High-Level Conference on AML/CFT of 30 September 2020, who noted that the absence of cash ceilings in many EU Member States facilitates laundering of proceeds for organised crime across the EU.

Impacts on coherence

The current situation raises issues of coherence in the application of the AMLD, as countries where cash ceilings have been introduced can only partly impose AML/CFT rules on traders in goods. In fact, already at the time of discussing the transposition of the 4th AMLD in 2018, some Member States underlined the difficulty to put in place obligations on traders in goods, as they considered that the huge range of sectors covered by this definition makes it almost impossible to check whether or not these obligations are applied. Many Member States declared at that time that they will favour a cash restriction for sums above EUR 10 000 instead of an obligation to apply AML/CFT measures for traders in goods.

Impacts on the level-playing field

Diverging national restrictions entail distortions of competition in the internal market. The 2017 study supporting the Commission report on restrictions on cash payments across the EU already highlighted negative impacts for businesses from the current situation. Certain business sectors in countries with cash payment restrictions are negatively affected to the benefit of their competitors in neighbouring countries without such restrictions, who take advantage of criminals forum shopping. The European Federation of Jewellery's contribution to the public consultation on the AML/CFT Action Plan noted that the Belgian jewellery sector alone estimates a loss of revenue by

20-30% as a result of this divergence in national measures. The Federation called for the introduction of a limit to cash transactions of EUR 10 000 at EU level, which it considers consistent with the current threshold applied to cash controls.

4. Options to address this problem

Several options could exist to address the negative impacts of a lack of coherent approach to limitations of cash payments.

Option 1: further enforce the current AML/CFT framework

This option would consist of the status quo, as described in the previous section, but with an enhanced control that traders in good apply AML/CFT measures adequately. This option would require a significant amount of additional human resources to be devoted to supervisory tasks across the EU, whom would be tasked with supervising a population of operators in constant evolution. Due to the anonymity of cash, even a more stringent application of AML/CFT rules would not deliver the desired outcome as the traders might find it challenging to identify when situations are suspicious without any risk of tipping off their clients. As a consequence, it is unlikely that this option would see FIUs receive reporting of any additional value than at present, which would allow them to produce financial intelligence of a certain quality to trigger investigations. Moreover, by the time this is done, the goods might have already left the country or changed in nature, as the above example shows.

Option 2: introduce an EU-wide limit to cash transactions of EUR 10 000, while allowing Member States to set a lower threshold

As mentioned in the previous section, the majority of respondents to the public consultation favoured the introduction of a limit to cash transactions across the internal market as a means to strengthen the EU AML/CFT framework. The introduction of such limit would provide a more harmonised approach across the internal market, reduce the inefficiencies of the current AML/CFT framework by lifting obligations on traders in goods and level the playing field among businesses, whilst not calling into question legal tender status of euro banknotes.

This option is also supported by respondents to the public consultation. Two thirds of those who had an opinion on this matter supported introducing cash limits as an effective way to counter money laundering.

Moreover, such limit would be consistent with existing thresholds for cash control and would ensure that vulnerable consumer groups are not adversely impacted by setting a sufficiently high ceiling to cater for their needs.

This option would also allow Member States to maintain lower limits already in place, recognising that national specificities might justify lower thresholds and includes the need to carry out a more in-depth assessment with a view to reviewing, in the medium term, the threshold set at EU level. This option would also allow Member States to

maintain as obliged entities specific sectors that are exposed to high ML/TF risks, in line with Annex 6.

Option 3: Introduce an EU-wide limit to cash transactions lower than EUR 10 000

The diverging national restrictions raise questions as to whether this allows the bypassing of national cash payment limits, and therefore decreases their efficiency[132]. This option would provide a more harmonised approach across the internal market, levelling the playing field among businesses and reducing opportunities for criminals to use cash to launder their illegal proceeds.

The Commission is currently working towards a thorough assessment of the introduction of an EU-wide limit lower than EUR 10 000, which analyses the matter in relation to broader aspects than AML/CFT such as tax evasion. Any threshold below EUR 10 000 would need to be carefully chosen taking into account the need to ensure financial inclusion, particularly of the most vulnerable citizens, the level of financial innovation across EU Member States and any adverse effect that such threshold might have on the proportionate and compatible with the legal tender status of euro banknotes.

While this might be preferable in the medium term, it would require further analysis before a proposal can be made. In the meantime, criminals would continue to be able to take advantage of the current situation to use cash to launder the proceeds of their illegal activities.

Based on the above, the preferred option at this stage is option 2, without prejudging on a subsequent proposal at a later stage based on option 3 that could go further into lowering and further harmonising the threshold.

5. **Proportionality of the proposed measure**

The Court of Justice of the European Union (the "Court") has established case law[133] acknowledging that the combating of money laundering constitutes a legitimate aim for justifying a barrier to the fundamental freedoms guaranteed by the Treaty.

Further, recital 19 of Council Regulation No 974/98 on the introduction of the euro explains that any limitations on payments in notes and coins, established by Member States for public reasons, are not incompatible with the status of legal tender of euro banknotes and coins, provided that other lawful means of payment for the settlement of monetary debts are available.

This status and its interaction with individual fundamental rights has been examined recently by the Advocate-General Pitruzzella[134] who opines that "*the Union does not*

[132] Conclusions of COM(2018)483 final (see p.8) and footnote 19 of the Action Plan (C(2020) 2800 final): Further targeted assessment of this matter will be explored in the course of 2021.
[133] Judgment of 31 May 2018, *Zheng*, C 190/17, ECLI:EU:C:2018:357, para 38; Judgment of 25 April 2013, *Jyske Bank Gibraltar*, C 212/11, ECLI:EU:C:2013:270, para 64; Judgment of 30 June 2011, *Zeturf*, C 212/08, ECLI:EU:C:2011:437, para 45-46

provide for an absolute right to payment in cash in all cases" and while "*EU law gives rise to a subjective position in which cash can be used for payments with the effect of releasing the debtor (...) it would still be (...) a subjective position which certainly does not feature in the catalogue of fundamental rights guaranteed by EU primary law*."

However, the Advocate stipulates that "*a direct link between cash and the exercise of fundamental rights does exist in cases where there is a social inclusion element of the use of cash (....), [specifically for vulnerable individuals for whom it is] only form of accessible money and thus the only means of exercising their fundamental rights linked to the use of money*"[135]. Therefore, social inclusion element should be used as the only test for determining the proportionality of the ceiling. In the case before the CJEU, the cash payments were not acceptable at all (for the payment of the radio and television licence fee), but since the social inclusion element was absent, even such absolute restriction on use of cash was deemed acceptable and proportionate.

The proposed threshold of EUR 10 000 would ensure that the restriction on the use of cash in transactions within the Union does not impede the exercise of fundamental rights by Union citizens that do not have access to alternative means of payment, and does not pose a disproportionate limitation of the freedom of movement of capital and freedom to provide services by Union citizens and businesses. As the tables below show[136], in most Eurozone Member States cards or other methods of payment are already preferred to cash for transactions above EUR 100. This trend remains consistent over time. In addition, in most of the countries where a majority of payments are carried out in cash also above the EUR 100 threshold[137], restrictions to the use of cash for large payments already exist. At the same time, as noted in a research paper by , there are limited social downsides to implementing large cash thresholds since, as shown, the overwhelming majority of legitimate cash transactions are below the levels at which cash thresholds would be imposed and high-value cash transactions that are not motivated by illegal purpose appear to be rare and only relevant to a small, wealthy proportion of the population.[138]

---

[134] Opinion of Advocate-General Pitruzzella of 29 September 2020, *Hessischer Rundfunk,* C- 422/19 and C- 423/19, ECLI:EU:C:2020:756, para 133

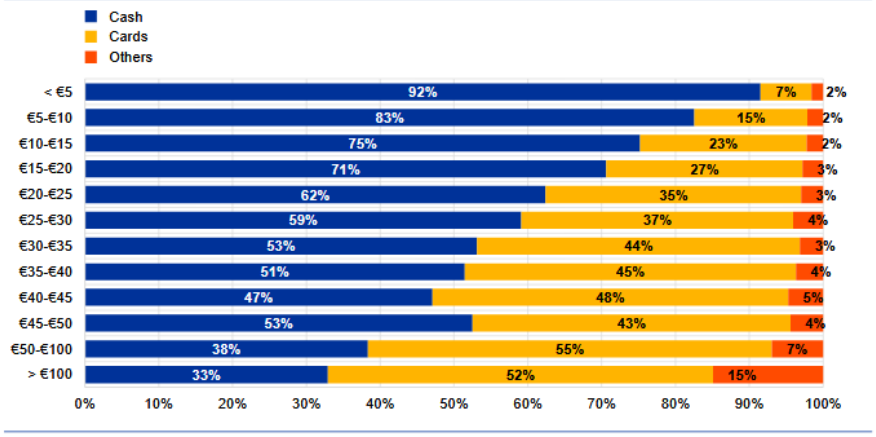
[135] Ibidem, para 134

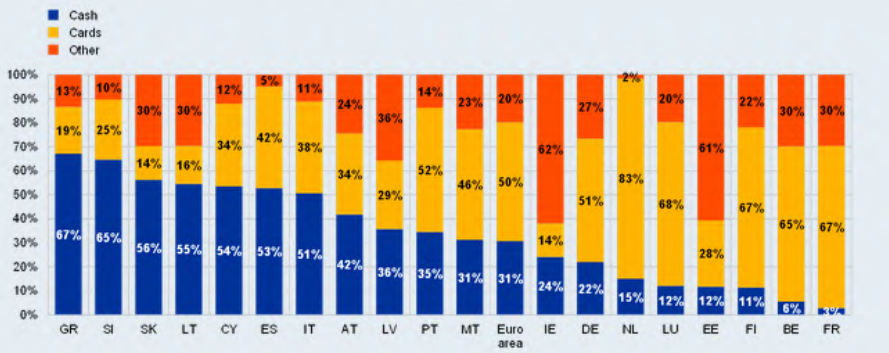
[136] Study on the payment attitudes of consumers in the euro area (SPACE), https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf?05ce2c97d994fbcf1c93213ca04347dd

[137] https://www.ecb.europa.eu/pub/economic-bulletin/articles/2018/html/ecb.ebart201806_03.en.html#toc4

[138] Peter Sands, Haylea Campbell, Tom Keatinge and Ben Weisman, *Limiting the Use of Cash for Big Purchases Assessing the Case for Uniform Cash Thresholds*, Mossavar-Rahmani Center for Business & Government (Harvard Kennedy School), M-RCBG Associate Working Paper Series No.80, September2017.

Number of transactions per value range and payment instrument



Transaction values by instrument and country for POS transaction amounts greater than €100

(percentage of total POS transactions > €100; value of transactions)