EUROPEAN
COMMISSION

Strasbourg, 5.7.2016
SWD(2016) 223 final

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

Proposal for a Directive of the European Parliament and the Council

amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC

{COM(2016) 450 final}
{SWD(2016) 224 final}

Table of Contents

CONTEXT AND INTRODUCTION

This impact assessment, proposing modifications to Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, consists of two parts.

Part 1 relates to five targeted amendments to this Directive to strengthen the EU's existing framework to fight terrorism and terrorist financing.

Part 2 concerns targeted amendments to this Directive to enhance transparency of beneficial owners of corporate entities and trusts.

PART I

1. BACKGROUND AND POLICY CONTEXT

On 20 May 2015, a new framework on anti-money laundering and counter-terrorist financing ("AML/CFT") was adopted. These new rules are, to a large extent, based on the international standards issued by the Financial Action Task Force (FATF)[1] and consist of:

(i) Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("4AMLD"), and

(ii) Regulation (EU) 2015/847 on information accompanying transfers of funds ("FTR").

The transposition date for the 4AMLD and the entry into force of the FTR is 26 June 2017.[2] Consequently, the transposition is ongoing in the vast majority of Member States.

The challenge for the AML/CFT framework is to ensure that the EU rules – and their enforcement – keep pace with evolving trends, developments in technology and the seemingly limitless ingenuity of criminals to exploit any gaps or loopholes in the system.

The recent terrorist attacks – which took place only few months after the adoption of the 4AMLD - underline the need for the EU to step up further its fight against terrorism and terrorism financing. Terrorist organisations and individual terrorists need financing in order to maintain their networks, recruit and supply terrorist fighters, and commit terrorist acts. Cutting off sources of finance, making it harder to escape detection when using these funds, and using any information from the financing process to best effect makes a powerful contribution to the fight against terrorism. Although the challenge of how to tackle terrorist financing is not new, new trends have emerged, seen in particular in terrorist organisations such as the Islamic State of Iraq and the Levant (ISIL) and among foreign terrorist fighters.

The above led to a reflection on the new challenges and threats posed by terrorist financing. In particular, this includes discussions at the FATF which raised, in a session in December 2015, the need to ensure sufficient powers and information-sharing among authorities to prevent against the risks posed by terrorist financing.

This has resulted in the Commission examining some policy options aimed at ensuring Financial Intelligence Units (**"FIUs")** cooperate with one another and have timely access to relevant information, amongst others through the use of a centralised bank account register or equivalent mechanism. Some ambiguity relating to FIU powers and cooperation has also recently been highlighted through Commission transposition workshops for the 4AMLD. The EU has also been criticised in recent months about shortcomings relating to FIU cooperation, following both the Paris and Brussels attacks.

While the 4AMLD prevents the use of the traditional financial system for the purposes of money laundering and terrorist financing, some services are becoming increasingly popular as alternative financial systems and remain outside the scope of EU legislation or benefit from exemptions that may no longer be justified. Innovation in financial services and technological

[1] The FATF is the most important international standard setter for AML/CFT. The European Commission and 15 Member States are Members of FATF and the remaining 13 are members of "MONEYVAL", the FATF-style regional body that conducts self and mutual assessment exercises of the AML/CFT measures in place in Council of Europe member states.

[2] In its Action Plan to strengthen the fight against terrorism financing of 2 February 2016, the Commission called on Member States to bring forward the date for effective transposition of 4AMLD to Q4 2016.

change, for all their benefits, create new opportunities which may be abused to conceal terrorist financing.

The attacks raised question-marks about the risks relating to anonymity for instruments which fall partially or wholly outside the scope of the EU rulebook. It is essential that the AML/CFT framework evolves to respond to new and emerging threats and that preventive measures are put in place to address existing gaps before those risks materialise. Concern emerged, in particular, with regard to **prepaid cards** which were used in the Paris attacks to book hotels and rent cars. Although prepaid cards present important economic benefits, their use in terrorist attacks raises the question about the take-up of such instruments and how their use should expand safely vis-à-vis other fully regulated alternatives (credit and debit cards).

For **virtual currencies**, the policy problem is similar, relating again to anonymity. Some Member States have reported that they have seen money laundering issues arise with respect to virtual currencies and see a possibility of these being used to fund terrorism. Many warnings have been made by international authorities about these risks, but they came too late in the 4AMLD negotiation process to be integrated into this instrument. Since then, a large number of Member States have taken steps unilaterally (or plan to) in order to regulate virtual currencies. Contacts with the virtual currency industry also indicated that a large part of the sector would welcome EU legislation in the field AML/CFT.

Finally, industry in particular sees value in harmonising the **enhanced due diligence that should be applied to high-risk third countries**. Feedback from industry highlighted inconsistencies across the EU for transacting with high-risk jurisdictions adding regulatory cost and complexity, and creating reputational concern about doing business with such territories.

Although none of the abovementioned subjects are really new - some of them have even been debated during the negotiations but were not withheld as there was at that time no sense of urgency - the terrorist attacks that took place in the aftermath of the adoption of the 4AMLD made both the Member States and the Commission conscious of the need to address these issues without delay, knowing that the ink of the 4AMLD was still drying.

The abovementioned recent game changers also show that money laundering, terrorist financing and organised crime remain significant problems which should be addressed at Union level. Some Member States already voiced their intention to take action in the abovementioned areas. However, uncoordinated action may reduce the good functioning of financial intelligence at EU level, and create gaps or weak spots that can be exploited by criminals and terrorists to channel their funds in and out the EU financial system, thus threatening the good functioning of the Internal Market. Taking into account the above and the Conclusions of the extraordinary JHA Council of 20 November 2015 and of the ECOFIN of 8 December 2015, the Commission published on 2 February 2016 a Communication[3] with an Action Plan to further step up the fight against the financing of terrorism. The Action Plan builds on existing EU rules to adapt to new threats and seeks to update EU policies in line with international standards.

The Action Plan focusses on **two main strands** of action:

- tracing terrorists through financial movements and preventing them from moving funds or other assets, and ensure that financial movements can wherever possible help law enforcement to trace terrorists and stop them from committing crimes;

[3] COM (2016) 50 final.

– disrupting the sources of revenue used by terrorist organisations, by targeting their capacity to raise funds.

One of the key actions of the Action Plan concerns the commitment of the Commission to present – at the latest by the second quarter of 2016 – legislative proposals to amend the 4AMLD in five specific and targeted areas:

– Enhanced due diligence measures/counter-measures with regard to high-risk third countries

– Virtual currency exchange platforms

– Prepaid instruments

– The access of Financial Intelligence Units (FIUs) to – and exchange of – information (to strengthen FIU powers and cooperation)

– The access of FIUs to centralised bank and payment account registers or electronic data retrieval systems

The aim of these amendments is to contribute to the first strand of the Action Plan: the amendments will further strengthen the existing legal AML/CFT framework[4], by (i) taking preventive steps with respect to anonymous instruments that may be used by terrorists and (ii) enhancing the transparency of financial streams linked to terrorism. Insight into terrorist fund transfers, which will be helped in particular by strengthening the powers of FIUs, will not only contribute to the freezing and seizure of such funds, but will also help to identify and unravel the terrorist networks and the individuals involved in these networks, thus contributing to the prevention of terrorist acts.

These five proposed amendments can also be directly linked to a number of other initiatives of the Action Plan, such as for example (i) the adoption of the EU list of high risk third countries, (ii) the reinforcement of the cooperation between FIUs through appropriate measures (FIU mapping), (iii) the legislative proposal harmonising money laundering criminal offences and sanctions, and (iv) the exploration of the possibility of introducing a self-standing legislative instrument to allow for a broader consultation of bank and payment account registers, beyond the scope of the 4AMLD.

On 12 February 2016, the ECOFIN Council called on the Commission to submit its amendments as soon as possible and no later than Q2 2016.

2. PROBLEM DEFINITION

While the recent amendment of the EU AML/CFT framework presents a major step forward in the prevention of money laundering and terrorist financing ("ML/TF"), by integrating the 2012 FATF standards into EU law, the latest terrorist attacks have shown that further steps to improve this framework are needed, especially (but not exclusively) where the detection of TF flows is concerned. Therefore, and notwithstanding the fact that the transposition of the Directive is still ongoing, the Commission decided on 2 February 2016 to re-open the 4AMLD on the aforementioned five specific issues.

These issues should be seen as stand-alone areas of action, based on recent experience and the wide-ranging discussion that has followed the terrorist attacks in Europe. But they can also be

[4] They should not affect the ongoing transposition of the 4AMLD.

viewed as inter-related, in that they collectively strengthen the level of prevention across the EU against terrorist financing.

All five initiatives will contribute to lifting/reducing of anonymity or enhancing transparency of criminal and terrorist financing flows, and will therefore directly or indirectly improve financial intelligence at EU level and protect the EU Internal Market against ML and TF threats. Moreover, the two initiatives regarding FIUs, will also directly improve financial intelligence (including exchange of information) at EU level.

Consequently, they will cumulatively ensure that the regulatory perimeter is appropriately drawn to tackle unacceptable levels of anonymity and to ensure that there is sufficient oversight, powers, and cooperation to ensure that public authorities are able to credibly defend the EU from the risks it faces.

2.1 Problem 1: Suspicious transactions involving high-risk third countries are not efficiently monitored due to unclear and uncoordinated customer due diligence requirements

2.1.1 Context

The risk based approach is a cornerstone principle of the AML/CFT framework and is fully implemented in the context of the 4AMLD. This principle is essential to an efficient allocation of resources when applying AML/CFT rules, by ensuring that measures to prevent or mitigate ML/TF are commensurate with the risks identified[5].

Nevertheless, the 4AMLD has recognised specific situations where the risk based approach is to be complemented with a common approach regarding enhanced measures to be applied by all obliged entities. This is the case for instance for cross-border correspondent banking relationships, for business relationships with politically exposed persons, or when dealing with natural or legal entities established in third countries identified by the Commission as high-risk third countries. In all these situations, obliged entities shall apply enhanced customer due diligence measures (ECDD measures).

At FATF level, the geographical/country risk is defined through two FATF public documents that are issued three times a year.[6] At European level, the geographical/country risk is one of the factors to be considered when conducting the risk assessment.[7] The identification of high-risk third countries is ensured at several levels:

- At the level of obliged entities, where risks factors related to countries or geographical areas may form part of their risk assessment
- at Member State level, where risks factors related to countries or geographical areas may form part of their national risk assessment

---

5 Following the risk-based approach, where the risks identified are high, Member States shall require from their obliged entities to apply ECDD measures, and where the risks are lower, they may decide to apply simplified due diligence measures only.

6 The FATF's "Public Statement" identifies:

- countries or jurisdictions with such serious strategic deficiencies that the FATF calls on its members and non-members to apply counter-measures, and
- countries or jurisdictions for which the FATF calls on its members to apply ECDD measures proportionate to the risks arising from the deficiencies associated with the country. The statement "Improving Global AML/CFT Compliance: Ongoing process" identifies countries or jurisdictions with strategic weaknesses in their AML/CFT measures but that have provided a high-level commitment to an action plan developed with the FATF.

7 See articles 8(1), 9, 17 and 18, and Annexes II and III of Directive (EU) 2015/849 (4AMLD).

– at European Union level, where the Commission has to identify high-risk third countries via delegated acts. The list of the Commission shall be established taking into consideration strategic deficiencies in the following areas: (i) the legal and institutional AML/CFT framework in the third county; (2) the powers and procedures of the third country's competent authorities for preventing ML/TF; and (iii) the effectiveness of the AML/CFT system in addressing ML/TF risks in the third country. The Commission will take into account relevant evaluations, assessments and reports drawn up by international organisations and standards setters, such as FATF in particular. This list will complement the lists adopted at national and sectorial level.

For higher risk business relationships, the FATF recommendations give some examples of ECDD measures[8] that can be applied by countries and obliged entities to mitigate the risks. In the case of such high-risk third countries, the business relationships may also be subjected to counter-measures[9] in the event that the country concerned has not demonstrated any commitment to improve their AML/CFT regime and presents "on-going and substantial ML/TF risks for the international financial system".

While the ECDD measures consist mainly in an enhanced monitoring of transactions (including on the customer, the purpose of the business relationship or the source of funds) and constitute the basic requirements to apply when dealing with countries presenting strategic deficiencies in their AML/CFT regime, the counter-measures have stronger effects, since they range from systematic reporting mechanisms, to a prohibition against establishing subsidiaries, to the limitation of business relationships or financial transactions (see also Annex 4).

2.1.2 The problem

Unlike the FATF recommendations, the 4AMLD does not prescribe the nature of the ECDD measures or counter-measures that shall be applied by obliged entities and Member States towards high-risk third countries designated by the Commission. It only refers to a general requirement to apply ECDD measures in such circumstances. Furthermore, no reference is made to situations where counter-measures shall be applied. The 4 AMLD puts more emphasis on clarifying the factors to be considered (such as geography, customer type, delivery channel etc.) to apply either ECDD or simplified customer due diligence measures, than on clarifying the nature of these ECDD measures.

In addition to the uncertainty regarding when ECDD measures shall apply, this approach fails to provide a common, global response by the EU to the risk posed by high-risk third countries, even though such countries pose a common risk across the Internal Market. In particular:

– some national AML/CFT regimes already provide for a complete set of requirements related to transactions involving high-risk third countries, i.e. the requirement to apply ECDD measures to high-risk third countries, as well as the nature of those ECDD measures.

Example 1: The AML/CFT law of Member State X states:

[8] See para 20 of the Interpretative Note to FATF Recommendation n°10 – page 65 (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

[9] See para 2 of the Interpretative Note to FATF Recommendation n°19 – page 79 (http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf)

"When dealing with natural or legal entities established in a third country identified by (decree/law n°...) as high-risk third countries, obliged entities shall apply one or all of the following ECDD measures:

a) additional information on the customer

b) additional information on the intended nature of the business relationship

c) information on the source of funds or source of wealth of the customer

d) information on the reasons for the intended or performed business relationship

e) approval of senior management to commence or continue the business relationship

f) enhanced monitoring of the business relationship

g) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards"

– other national AML/CFT regimes are less detailed, keeping a general reference to ECDD measures applicable to FATF lists of high-risk third countries with no further indication as to the type or nature of the measures that should be applied.

Example 2: The AML/CFT law of Member State X states:

"When dealing with natural or legal entities established in a third country identified by FATF as high-risk third countries, obliged entities shall apply ECDD measures.

– other national AML/CFT regimes are silent as regards the legal framework applicable to high-risk third countries. In such cases, the management of high-risk third countries is left to the obliged entities' discretion.

Example 3: The AML/CFT law of Member State X states

"When assessing the risks of ML/TF, obliged entities shall take into account the geographical risk factors".

2.1.3 The problem drivers

The lack of clear provisions concerning the nature and type of ECDD measures or counter-measures that should apply for dealings with high-risk third countries creates legal uncertainty regarding the specific steps that obliged entities should take to ensure adequate and robust due diligence. It also leads to discrepancies between different sets of national legislation (whereby more lenient legislation may potentially allow terrorists or criminals groups to transfer illicit funds more easily). These 'gaps' between national laws are much more worrying when the strategic deficiencies relating to a particular high-risk third country refer to basic and fundamental elements of an AML/CFT system (i.e. criminalisation of ML/TF, implementation of customer due diligence, requirements related to record keeping or requirements to report suspicious transactions), which merit specific and efficient monitoring.

2.1.4 The effects of the problem

In the absence of unambiguous and detailed provisions related to ECDD measures, obliged entities may fail to detect efficiently suspicious transactions involving third countries, recognised at EU level as being risky, because of the inadequacy of their monitoring process. In turn, this may also incur reputational risk.

The variety of national practices towards high-risk third countries may also challenge the added-value of the EU listing process of those countries, provided by Article 9 of the Directive, if the same level and type of ECDD measures is not ensured. Without a corresponding harmonised approach, the EU listing may not achieve its desired effect:

– the lack of clear requirements may weaken the level of controls applied to transactions involving high-risk third countries in some Member States, resulting in suspicious transactions going undetected;

– criminals would have the possibility to exploit potential loopholes or take advantage of more lenient legislation through regulatory arbitrage.

Example 4 (hypothetical): In Member State A, obliged entities shall only obtain additional information on the customer when dealing with natural or legal entities established in a third country identified as high risk. In Member State B, in the same circumstances, obliged entities shall apply the full range of ECDD measures (i.e. obtaining additional information on the customer, on the intended nature of the business relationship, on the source of funds, on the reasons for the intended or performed transaction, as well as obtaining senior management approval to commence the business relationship and an enhanced monitoring of the business relationship).

Terrorists or criminals established in the designated high-risk third country C will decide to place or transfer proceeds of crime through credit or financial institutions governed by less stringent legislation, i.e. Member State A. Indeed, in Member State A the terrorist or criminal will be asked to provide additional information on the status of his customer only (where fake documents may easily be used), while in Member State B more complete enhanced monitoring (sources of funds, intent of the business relationship, senior management approval) will be less easy to circumvent. Under this scenario, the detection of a suspicious transaction will be easier in Member State B.

– it may create an unlevel playing field between obliged entities when national requirements are not the same and do not involve the same investment from an IT or administrative point of view. The more ECDD measures that are applied, the more filters and red flags may be included in the monitoring system of an obliged entity.

Example 5 (hypothetical): When opening an account for Mr xxx established in a designated high-risk third, bank A will only require from Mr xxx to fill in an extended questionnaire to have additional information on him, while bank B will require from Mr xxx to fill in several questionnaires to have additional information on him, the source of his funds, and the purpose of his transactions. Depending on the level of the ECDD requirements, bank B will also have to ask for the approval of senior management of the bank, via a formal procedure.

2.1.5 The size of the problem/Baseline scenario

The number of affected obliged entities depends on their level of business exposure with high-risk third countries. Financial institutions such as credit institutions, payment institutions, electronic money institutions and money value transfer services are the key actors concerned and can reach a very high number at EU level. Other professional sectors such as gambling service providers, legal professionals or insurance service providers are also relevant sectors exposed to this problem, but to a lesser extent given the nature of their activities.

Business exposure to high-risk third countries

Do you currently conduct business relationships or transactions with clients that are natural or legal persons from countries that are identified by the FATF as presenting AML/CFT strategic deficiencies?	81% of positive responses
What is the volume of activities undertaken by your institution/group, directly or via branches or subsidiaries, in countries that are identified by the FATF as presenting AML/CFT strategic deficiencies?	"very low", "negligible", "insignificant expression", "1-4 per year", "289 customers", "less than 1%", "1,56% of the customer base".
One specific case: money remitters - business exposure - volume of activities	- money remitters located within the EEA are not so much directly exposed (i.e. through having direct business relationships with entities/persons from such countries). However, as these remitters are generally part of a worldwide financial group, they are often indirectly exposed. - data related to the volume of activities are not available

***Source**: Extracts from written consultation organised in February 2016 – 21 respondents' professionals federations or organisations*

It depends also on the scope of high-risk third countries at stake and the circumstances when ECDD measures are applied.

As regards the scope of high-risk third countries concerned, obliged entities shall rely on several sources, potentially cumulatively, i.e.:

a) the countries listed by the Commission which have strategic deficiencies in their national AML/CFT regimes posing significant threats to the financial system of the Union[10];

b) the countries listed by the FATF which are identified in the two FATF public documents of February 2016[11];

c) the countries listed by Member States or obliged entities themselves because of the strategic deficiencies identified in the context of their national or sectorial risk assessment.

As regards the ECDD measures applied towards designated high-risk third countries, obliged entities tend to use the examples of ECDD measures provided by the FATF recommendation but not in the same circumstances:

a) some obliged entities systematically require additional information on the customer when dealing with high-risk third countries, while others apply this requirement on a case-by-case basis;

b) some obliged entities rely on external sources to check the source of funds while others use extensive questionnaires addressed to the customer;

c) some obliged entities systematically escalate the decision to undertake the transaction to their senior management or the money laundering risk officer while others rely on senior management approval only in specific circumstances, such as where politically exposed persons are concerned by the transaction.

All 28 Member States are potentially impacted by this problem as they are all covered by the requirements of 4AMLD.

2.2 Problem 2: Suspicious transactions made through Virtual Currencies are not sufficiently monitored by the authorities, which are unable to link identities and transactions

2.2.1 Context

[10] Article 9 of the 4AMLD defines the criteria that the Commission shall follow to draw up its list, in particular on the basis of relevant evaluations, assessments or reports drawn up by international organisations and standards setters with competence in the field of preventing ML/TF (i.e. mainly FATF).

[11] The FATF's "Public Statement", identifies countries or jurisdictions with such serious strategic deficiencies that the FATF calls on its members and non-members to apply counter-measures, and countries or jurisdictions for which the FATF calls on its members to apply ECDD measures proportionate to the risks arising from the deficiencies associated with the country. The statement "Improving Global AML/CFT Compliance: On-going process" identifies countries or jurisdictions with strategic weaknesses in their AML/CFT measures but that have provided a high-level commitment to an action plan developed with the FATF. Currently, 13 countries are listed in FATF documents, among which North Korea and Iran are submitted to counter-measures.

Virtual currencies ("VCs") are a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a fiat currency[12] ("FC"), but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically[13]. There are hundreds of VCs on the market and the most well-known is "Bitcoin" which accounts for 90% of the total market capitalisation of VCs.

Various stakeholders are involved in the VC industry, with the main actors being:

- users (investors, merchants, consumers using VCs to make payments or buy from merchants accepting VCs)
- miners, that validate transactions and receive VCs as rewards for their work
- wallet providers where users may hold their VC accounts and which can be divided into two categories: software wallets providers (i.e. applications to access VC networks and providing public information such as balances of VCs), and custodial wallets providers (which hold the private key of VC users and have control over VCs. We would include multi-signature wallets under this category, i.e. wallets for which the private keys are shared by more than one user in addition to the wallet provider).

  Compared to traditional financial services, custodial wallet providers that provide VC wallets to their users can be seen as financial institutions that provide bank or payment accounts to their customers. When such fund transfers are done between financial institutions, this is regulated by the Fund Transfer Regulation[14]. However, the same transfer in VCs – trough VC wallets held by VC wallet providers – is unregulated.
- exchange platforms, engaged in the exchange of VCs for FCs, FCs for VCs, or VCs for other brands of VCs. Compared to traditional financial services, they are the "bureau de change" of the virtual currency world. Automated Teller Machines (ATMs) are included under this category.

2.2.2 The problem

VCs have various characteristics that may allow them to be used as alternative channels for criminals looking to transact or transfer money electronically (see drivers). The main issue is their **anonymity.**

The story[15] of Ali Shukri Amin who provided instructions over Twitter on how to use Bitcoin to mask the provision of funds to Daesh is an example of the risks brought by VCs. Various cases involving the use of VCs to buy guns have also been reported[16].

Example 6: Amin tweeted a link to an article he had written entitled "Bitcoin wa' Sadaqat al-Jihad" (Bitcoin and the Charity of Jihad). The article discussed how to use bitcoins and how jihadists could utilise this currency to fund their efforts. The article explained what bitcoins were, how the bitcoin system worked and suggested using Dark Wallet, a new bitcoin wallet, which keeps the user of bitcoins anonymous. The article included statements on how to set up an anonymous donations system to send money, using bitcoin, to the mujahedeen.

Source: extract from the FATF report - Emerging Terrorist Financing Risks – October 2015

[12] i.e. a currency established as money by government regulation or law.

[13] Definition extracted from "EBA Opinion on virtual currencies" – 4 July 2014 – page 5.

[14] Regulation 2015/847.

[15] See case study 23 of FATF Report – "Emerging Terrorist Financing Risks" – October 2015 – page 36.

[16] http://www.coindesk.com/us-arms-trader-allegedly-used-bitcoin-for-purchases/

Moreover, VC market players, be they users (traders, suppliers, customers), 'miners', currency exchange platforms or wallet providers are currently not regulated at EU level nor in most EU Member States at national level. As a consequence, no one is under the obligation to report any suspicious transactions to an FIU (even though some do it spontaneously) and authorities lack information on such transactions.

Creating measures that cover one or various market players who act as major gateways to the VC environment could help lift, at least partially, this anonymity. These market players could perform user identity checks as well as report suspicious transactions. Virtual currency exchange platforms (including some ATMs equipped with such functionalities) where one can buy or sell virtual currency units in exchange for fiat currencies, could play that role of gatekeeper between the virtual sphere and the real 'world'. The same approach could apply to custodial wallet providers which offer in the virtual sphere the equivalent of a bank account where to store one's virtual currencies. Miners, however, do not fall under this category, as they have no specific interactions with users. Moreover, most of them are located in China which would make any initiative largely impossible to enforce. Users' identity is of difficult access and a number of users may be attracted primarily by the anonymity offered by virtual currencies and could therefore be more reluctant to willingly contribute to the sanitisation of the market. However, there may be other users primarily interested by the economic dimension of that market, because it constitutes a support for (speculative) investment or offers lower transaction cost for cross-border payments, who might be ready to divulge their identity in order to bring more transparency in the market, contributing thereby to improving its reputation and in turn its greater use.

Although the use of VCs is currently still limited, such currencies create new economic opportunities for online payments. Therefore, any new policy in this field should respect the test of necessity and proportionality, and be genuinely designed to protect specific public policy objectives.

2.2.3 The problem drivers

In contrast to traditional financial services, VC users' identities are unknown. Major VC schemes such as Bitcoin have anonymity by design. Attempting to find out users' identities requires enormous effort as no identity is linked to transactions. Authorities have to track transactions to a point where the identity may have been linked to an account or address (e.g. wallet providers or exchange platforms).

As VC users are not covered by any EU legislation and no AML/CFT requirements are imposed on market players that could trigger customer due diligence (unlike for more traditional financial services), authorities have to use other more complex techniques. These include tracking IP addresses to put an identity on an account, which generates certain costs (it would take several hours' labour to investigate and make associated requests to internet service providers).

Finally, VCs benefit from a growing network of acceptance (retailers online or offline, products and services available) and have numerous points of convertibility into FCs (through exchange platforms, ATMs or person-to-person transactions). As a consequence, the primary area of concern today is where VCs are exchanged for FCs and enter the real economy.

It should be noted though that the risks posed today may evolve as the network of acceptance of VCs continues to grow (see figures for number of wallets and estimations on the number of users and merchants accepting virtual currencies in Annex 5). There might come a point in

time when there will no longer be a need to convert VCs back into FCs if VCs become widely accepted and used.

2.2.4 The effects of the problem

The anonymity of VCs, their growing acceptance, and the capacity to go from the VC environment to the FC environment with ease, turn VCs into a potential vehicle for criminal activity (including ML/TF).

2.2.5 The size of the problem/Baseline scenario

Inaction at EU level could prompt measures to be taken at national level, leading to inconsistent approaches and regulatory arbitrage within the EU. Annex 5 provides an overview of the heterogeneous measures already taken or announced across the EU.

Continued increase of the usage of VCs will influence the potential consequences of the problem. Even though the full scale of misuse of VCs is unknown, its market value is already above €7 billion worldwide.

2.3 Problem 3: Current measures to mitigate ML/TF risks associated with anonymous prepaid instruments are not sufficient

2.3.1 Context

In Europe, the prepaid instrument market essentially is a prepaid card market. Prepaid cards started developing at the end of the 1990s as an alternative to debit cards (which require the existence of a payment account at a bank or a financial institution) and to credit cards (which require the card issuer to evaluate the cardholder's minimum level of creditworthiness).

Prepaid cards began as a device used to pay for goods and services where the issuer does not need to conduct any analysis on the cardholder's credit standing, and the cardholder does not have to bear the costs for opening and maintaining a payment account. There are basically two main categories of prepaid cards: 'closed-loop' prepaid cards, for purchases at a single merchant or among a limited network of merchants, and 'open-loop' / general purpose prepaid cards. General purpose prepaid cards are further divided into two sub-categories: reloadable cards and non-reloadable cards. Many of these cards need to be activated online to become operational.

The prepaid card market is partially subject to AML/CFT requirements today. The 3AMLD provides that holders of prepaid cards shall be subject to customer due diligence[17] (CDD) for non-reloadable cards with a storage exceeding €250[18] (for intra-EU use, up to €500 for domestic use) and for reloadable cards for yearly reloads in excess of €2500. As a consequence, a large part of the EU prepaid card market is already subject to customer due diligence. This is the case typically for travel cards – a substitute to travellers cheques – corporate cards, social benefit cards and for general purpose prepaid cards that are used like a

[17] A process entailing the identification and verification of the identity of the customer, to be conducted by "obliged entities" when entering into a business relationship with a customer or when executing certain financial transactions for the customer.

[18] This € 250 threshold results from an amendment of the initial threshold of €150 in the 3AMLD by the 2009 Second Electronic Money Directive. The main thrust of the 2nd EMD was to be market friendly in order to revamp an e-money market that had not really taken off. Increasing the €150 threshold to €250 was also a way to cater for inflation without having to regularly revise the Directive.

debit or a credit card (all the more so when linked to a bank account). The market segment of prepaid cards subject to CDD will be further extended by the 4AMLD which (i) reduces the exemption threshold for reloadable cards by introducing a monthly (maximum reload and maximum spending limit of €250) rather than a yearly limit beyond which CDD will have to be performed, and (ii) requires additional conditions for the cards (reloadable or not) to benefit from the CDD exemption, notably that the payment instrument is used exclusively to purchase goods and services (and not for peer-to-peer payments) and that the payment instrument cannot be funded with anonymous electronic money.

CDD has to be performed by the issuers of prepaid instruments covered by the Second Electronic Money Directive. Such issuers are regulated as 'obliged entities' under the 4AMLD. Card schemes[19] and distributors of prepaid instruments are outside the scope of both Directives.

2.3.2 The problem

The TF risk posed by prepaid cards is essentially linked to anonymous prepaid cards run on domestic or international schemes. These are general purpose non-reloadable cards with a nominal value of €250 or less, as well as those general purpose reloadable cards which can be reloaded up to €2500 over a year without being mandatorily subject to CDD. Although anonymity may be considered an advantage to protect the privacy of 'good-faith' users, privacy may also be misused to finance criminal activities. The key question is how to address the concerns raised by the anonymity of general purpose cards without wiping out the benefits that these instruments offer in their normal use (financial inclusion, protection against fraud, payment of social benefits), and shifting the risk to other less detectable means of payments, notably cash. Therefore, from a fundamental rights perspective, the question whether it is worth further regulating a fast-changing and potentially beneficial market deserves to be examined further, and the test of proportionality and necessity needs to be taken into account when assessing the options.

The issuance and acceptance of prepaid cards takes place under a regulated framework both within the EU and globally. In principle, prepaid card issuers – in accordance with European AML/CTF legislation – have to subject buyers of those cards to CDD. However, both the 3AMLD and the 4AMLD grant Member States the option to exempt from such requirements low nominal value cards or cards with a limited usage as these in principle present low ML/TF risks. Under the 3AMLD, all but three Member States decided to apply this exemption. In the context of the implementation of the 4AMLD, six Member States have already decided not to apply the exemption and seven have not yet taken a decision. The remaining 15 Member States will apply the exemption offered by the 4AMLD (which is stricter than under the 3AMLD, notably with regard to reloadable cards).

Even within a regulated environment, law enforcement authorities (in the US[20] and in Europe) have encountered misuse of prepaid cards[21] in relation to criminal activities (drug trafficking, human trafficking, prostitution etc.), illegal labour and tax evasion leveraging the anonymity offered by some of these cards.

---

[19] E.g. American Express, MasterCard, Visa.

[20] Board of Governors of the Federal Reserve System, "Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Access Cards" – 21 March 2016 – Page 2.

[21] FATF Report of October 2010 – "Money laundering using new payment methods".

Example 7: The investigation into the November 2015 attacks in Paris has revealed that a prepaid reloadable card issued in the EU was used for the rental of flats in Alfortville as well as the rental of cars for the commando. That card had been reloaded many times with individual reloads in excess of €750 EUR[22]. Whilst electronic means are traceable after-the-event (unlike cash) and thus it was possible to know that a given card was reloaded many times, if the card is CDD-exempt (as in this case), it is not possible to attach a name to the holder of the card.

The Belgian press[23] recently reported that Salah Abdeslam, one of the protagonists of the Paris attacks, had used an anonymous prepaid card to move around in Europe over a period of time before his arrest.

The concerns of the law enforcement authorities vis-à-vis the misuse of prepaid cards have been exacerbated as a result of the security shift that has followed the 2015 Paris attacks. The degree of anonymity subsisting in the prepaid card market, although significantly reduced under the 4AMLD, is not considered acceptable. Additional efforts are expected to further reduce anonymity in that sector, considering that the social convenience offered by prepaid cards does not have to necessarily equate with anonymity.

[22] Reloadable prepaid cards under the 3AMLD are not subject to CDD, until a threshold of €2 500 is reached.

[23] http://www.lesoir.be/1209582/article/actualite/belgique/2016-05-13/salah-abdeslam-utilise-une-carte-credit-anonyme-pour-se-deplacer

2.3.3 The problem drivers

Existing EU legislation follows a 'risk-based approach' on how to tackle ML and TF. On that basis, when meeting certain conditions, Member States are granted the possibility to exempt prepaid cardholders from CDD, which leads to anonymous transactions.

At the same time, CDD implies compliance costs and administrative burden for prepaid card issuers. Compliance costs could – if excessive – finally lead to the disappearance of products which (i) constitute an efficient alternative to cash, allowing their users to buy goods or services in non-face to face environments, in particular online, (ii) from an AML/CFT viewpoint, remain far more traceable than cash for *ex-post* investigations, even where exempted, and (iii) present a clear social interest (financial inclusion, protection against fraud, payment of social benefits). Restrictions could also lead to distribution through bank networks only, which might be an issue for the unbanked.

2.3.4 The effects of the problem

The anonymity of prepaid cards is seen as an asset by criminals, all the more so as the acceptance of prepaid cards in the Union is relatively high and their spread is widening.

Whilst prepaid cards are more traceable than cash in *ex-post* investigations, they are also less detectable physically. Where police or customs dogs are trained to detect bulks of bank notes, they cannot do so for plastic cards. Furthermore, for reloadable cards, where the money is not loaded on the card chip (i.e. in most cases), law enforcement authorities cannot know what amount of money is accessible via the card. This will however be addressed for part by the 4AMLD which imposes a €250 cap on general purpose reloadable prepaid cards both in respect of spending and reloading capacity.

2.3.5 The size of the problem/Baseline scenario

The exact size of the EU prepaid card market is difficult to assess as no public statistics are available. Based on industry estimates, the EU market in transaction value would represent about €19 to 20 billion (compared to €2 400 billion transaction value for debit and credit cards in the Union in 2014), of which about €11 billion relates to anonymous prepaid cards.

There are relatively abundant FATF typologies[24] on the misuse of prepaid cards for ML purposes. It is, however, not possible to provide a full scale as to their misuse in terms of transaction value compared to their legitimate use. At the same time, anonymity is used as a selling argument by a number of issuers[25] and this market segment, whilst relatively small, still represents a sizeable grey area.

Failure to act at EU level would lead to the persistence of a non-negligible regulatory and security gap in the EU framework. Member States have the option under EU law not to exempt prepaid cards from CDD. A higher number of Member States (six or seven) are

[24] FATF Report of October 2010 – "Money laundering using new payment methods".

[25] http://www.etreanonyme.fr/#!carte-prepayee/coiy. This French website used to promote the anonymity offered by prepaid cards until the end of 2015. It closed some time after the November 2015 Paris attacks. On internet, other websites can be found where anonymity is used as an argument to attract users (See e.g. https://www.sovereigngoldcard.com/offshore-blog/demystifying-anonymous-prepaid-cards).

contemplating doing so under the 4AMLD. At the same time, if the current exemption is not more strictly framed, as the appreciation of risk may vary across Member States, additional measures will be taken at national level to address the existing risk linked to the anonymity of prepaid cards.

These measures, uncoordinated, would lead to inconsistent approaches, a patchy Single Market and a risk of regulatory arbitrage between Member States depending on the strength of their AML/CFT rules vis-à-vis prepaid cards, with displacements of issuing activities.

To avoid or reduce the risk of circumvention related to the use of foreign prepaid cards in the EU, the adoption of similar standards by the FATF would be appropriate. In the meantime, conditions of equivalence might need to be defined in EU law to prevent the misuse in the territory of the Union of cards issued in jurisdictions with lesser AML/CTF requirements.

2.4 Problem 4: FIUs have limitations in the timely access to – and exchange of – information held by obliged entities

2.4.1 Context

FIUs are public authorities that collect and analyse information (a.o. suspicious transaction reports ("STRs")) they receive from obliged entities (e.g. credit and financial institutions) under the 4AMLD. The regulation of obliged entities under the 4AMLD aims to establish a mechanism to detect suspicious transactions and underlying criminal activity, in order to prevent and combat ML and TF. In the event that their analysis reveals a suspicion of ML or TF, FIUs are also responsible for disseminating the results of their analysis and any additional relevant information to competent (law enforcement) authorities. FIUs are also empowered to take urgent action, such as the suspension of financial transactions.

2.4.2 The problem

Some FIUs are not yet able to obtain additional information from obliged entities, unless the same obliged entity has previously filed an STR. As a consequence, those FIUs are not able to further analyse a suspicion of ML or TF, which hinders their capability. Similarly, it impedes effective cooperation between FIUs as some FIUs, in turn, cannot further process a request for information submitted by another EU FIU.

In addition, some FIUs do not directly have access to information held by obliged entities – but rely on a third party to access this information (e.g. prosecutor or judicial authority). Such indirect access increases the delay for the FIU in accessing information held by obliged entities. Such delays are particularly problematic where an FIU needs to rapidly access information in view of taking a decision for suspending/withholding consent for processing a transaction. Especially in cases involving terrorism financing, it remains of paramount importance that information flows quickly without undue delays. In practice, delays negatively affect cooperation between EU FIUs. Moreover, in some cases, the third party may impose further restrictions, conditions or limitations when such access is sought following a request from another EU FIU. As a consequence, some third parties are also in a position to refuse the provision of information following a request from an FIU of another Member State.

The abovementioned concerns and the demand to tackle them have been tabled by the Council on 20 November 2015, following the Paris terrorist attacks.

2.4.3 The problem drivers

The 4AMLD already provides that FIUs "shall be able to obtain additional information from obliged entities", and does not make any reference in this respect to the necessity of filing a prior STR. In this respect, the 4AMLD follows standards set by the FATF in its Recommendation 29 on FIUs (cf. text in Annex 6). However, the necessity of having a prior STR filing has been continuously questioned at international level, notably at the FATF. The latter recently confirmed that no prior STR filing was needed. However, it appears that differences in interpretation of the international standards in this field have impeded full effect of this provision across Member States.

Furthermore, as stated above, the procedures in place in certain Member States require a third party authorisation for the FIU to request information from obliged entities. This practice was reflected in the adopted wording of article 31(1) (b) of the 4AMLD which provides that obliged entities should provide the information to the FIU "directly or indirectly" at its request. Hence the provisions of the 4AMLD are insufficient in this regard.

2.4.4 The effects of the problem

The analysis function of an FIU is seriously limited if it cannot obtain additional information from an obliged entity in the event of a suspicion of ML/TF. It negatively impacts on its core functions and impedes effective cooperation and information-sharing with other EU FIUs. Similarly, the indirect access by FIUs to information held by obliged entities provokes further delays. The third party's authorisation may also be refused and hence a request from another FIU may not be processed.

Example 8: the following illustrative examples were provided by FIUs with regard to the effects of the problem:

- In several cases, other Member States' FIUs were unable to request and provide to FIU A the bank statements and data about authorised representatives and the ultimate beneficial owner because of domestic legislation. Those FIUs would have been able to do so if there was an ongoing criminal investigation or if the information was contained in the FIU database (i.e. a previous STR about the same case was filed to the FIU by an obliged entity).
- The FIU of country B received an STR from an obliged entity in country B concerning the transfer of €600 000 coming to the bank account of the foreign company AB from the foreign bank account of the same company. The representative of the company AB intended to withdraw money in cash. The bank postponed the transaction, performed CDD and filed an STR. The FIU of country B asked the FIU of country C to check the foreign bank account of the company AB and the origin of funds. The FIU of country C provided information that company AB and its bank account were not listed in the FIU database. The FIU of country C was not able to ask the bank to check the origin of funds. Due to the lack of information, financial funds were unblocked and paid to the representative of the company AB. After two weeks, the FIU of country B received information from foreign banks concerning the fraudulent origin of funds.
- For some FIUs, the access to financial information required a judicial procedure and, in this case, it is difficult to cooperate with administrative FIUs.
- The FIU of Member State F is not authorised to obtain additional information in the course of its analysis.
- The FIU of Member State G can obtain additional information in the course of its analysis if there is a domestic STR. However, a foreign FIU request (based on a STR in this other Member State) is not considered equivalent with a domestic STR for Member State G. Hence it does not trigger analysis or does not allow for exchange of information between those FIUs.

2.4.5 The size of the problem/Baseline scenario

FIUs have confirmed that the current practice has a disruptive effect on cooperation and impedes their effective work. It appears that a number of Member States have limitations regarding access to information and exchange of information between FIUs. Notably, even if only one FIU lacks those powers, this would undermine the EU's analysis capacity due to the high level of integration of the EU financial market.

FIUs have reported several cases where another FIU did not have the authority to obtain additional information from obliged entities. In addition, some FIUs were not in a position to reply to a counterpart's request because they did not have direct access to the information. In sum, FIUs are not able to access all the information they need and to exchange such information with other FIUs. Ultimately, this leads to situations where money launderers or terrorists may misuse the financial system without the FIU being able to intervene.

These problems have been reported for several years now. The Member States concerned have not voluntary changed those practices.

2.5 Problem 5: FIUs[26] lack access or have delayed access to information on the identity of holders of bank and payment accounts

2.5.1 Context

In order to adequately fulfil their duties, as stated under point 2.4.1 above, FIUs need to have – in a timely manner – a comprehensive picture of all financial transactions conducted by persons involved in suspicious transactions. In a number of Member States, information at national level allowing the identification of bank and payments accounts belonging to one person is fragmented and therefore either not accessible to FIUs at all, or not accessible in a timely manner.

2.5.2 The problem

Lack of access or delayed access to information on the identity of holders of bank and payment accounts by FIUs hampers the detection of financial flows relating to terrorism, both nationally and at EU level.

Certain Member States have put in place adequate mechanisms to tackle this problem - such as centralised banking registries or electronic data retrieval systems which contain/retrieve such information (as encouraged in recital 57 of the 4AMLD, and required by the FATF standards[27]). However, there is no obligation at EU level to do so. Moreover, not all Member States that currently have such mechanisms in place allow their FIUs to have access to those systems.

Therefore, in Member States which do not have such mechanisms in place, FIUs wanting to obtain a list of all the bank and payment accounts held by a person suspected of ML or TF need to formulate a "blanket request" to all credit and payment institutions in their country. This is time consuming and creates unnecessary cost (cf. table in Annex 7). It may also result in the dissemination of personal data in a non-targeted way to financial institutions, which can create problems from a data protection and fundamental rights perspective. Moreover, in most Member States, sending blanket requests is - from a cost and administrative perspective - simply not a feasible option. In such cases, this will lead to non-action by FIUs.

As a consequence, FIUs are unable to exchange relevant information relating to ML and TF with their EU and non EU-counterparts, which complicates cross-border preventative action. The latter is an essential component in the fight against ML and TF.

---

[26] It is worth flagging that this problem may also concern other competent authorities (such as for example tax authorities) mentioned in the 4AMLD.

[27] Recommendation 31 of the FATF Standards states *(...)" In addition, countries should have effective mechanisms in place to identify, in a timely manner, whether natural or legal persons hold or control accounts.*" (…).

Example 9:

The FIU of Member State (MS) A receives an STR with regard to a suspicious transaction conducted by Mr. X on a bank account in MS A. As Mr. X is a resident of MS B, the FIU of MS A informs the FIU of MS B of this information.

Hypothesis 1: MS B has a register enabling the FIU to identify the holders of bank and payment accounts. Upon receipt of the information from the FIU of MS A, the FIU of MS B will enter a query with regard to Mr. X in the register, and instantly receive the result. The search shows that Mr. X holds 2 bank accounts in MS B: one in bank Y, and one in bank Z. The FIU of MS B immediately contacts both banks and blocks the accounts, on which apparently money of criminal origin coming from a company O, having its registered office in MS C, was transferred. Law enforcement authorities seize the illicit funds on both bank accounts in MS B. Furthermore, the FIU of MS B informs the FIU of MS C of this information, thus allowing authorities in MS C to further investigate company O.

Hypothesis 2: MS B is a medium size country with a medium size financial sector. MS B does not have a register of accountholders, but the FIU of MS B sends out blanket requests to all bank and payment institutions in MS B. This procedure has a certain cost (cf. Annex 7 for the annual costs) and takes approximately 3 days to 1 week (first, the requests need to be sent out, then all financial institutions need to search their files to check if Mr. X is one of their clients, and finally, they all need to reply to the FIU whether Mr. X is one of their clients or not). By using the blanket requests, the FIU of MS B receives information showing that Mr. X holds 2 bank accounts in MS B: one in bank Y, and one in bank Z. The FIU of MS B immediately contacts both banks. Unfortunately, the day before, Mr. X has transferred the money from criminal origin on those two bank accounts to another account in MS D. Consequently, the money cannot be blocked/seized anymore. Also, Mr. X, alerted by the fact that his account in MS A was investigated by law enforcement authorities, informed company O in MS C of this, following which company O immediately closed down its bank account.

Hypothesis 3: MS B is a large country with a big financial sector. MS B does not have a register of accountholders, and its FIU does not use blanket requests, which are considered as unworkable, taking into account the costs and administrative burden linked to this technique for a country of that size. After having received info from the FIU of MS A, the FIU of MS B remains unaware of the accounts of Mr. X in MS B with banks Y and Z. Also, FIU B remains unaware of the fact that company O channels criminal money from MS C into these two accounts. Consequently, the FIU/law enforcement authorities of MS B cannot block/seize the funds on those two accounts, and Company O remains entirely undetected.

The need for FIUs to have a fast access to necessary information to perform their duties has also been tabled by the Council on 20 November 2015, following the Paris terrorist attacks.

2.5.3 The problem drivers

In order to adequately fulfil their duties, FIUs need to have – in a timely manner - the fullest picture of all financial flows relating to persons involved in suspicious transactions. The current European AML/CFT framework does not require Member States to set up mechanisms allowing FIUs to get timely access to information on the identity of holders of bank and payment accounts.

2.5.4 The effects of the problem

Delayed access, or non-access, to this information results in FIUs having no view or only a partial view on criminal or terrorist financial flows (cf. case example, hypothesis 2 and 3) by which to analyse ML/TF suspicions. As (part of) the illicit funds remain undetected, those funds cannot be blocked or frozen, and remain available in the financial system in order to be laundered or used for terrorist activities. Finally, FIUs are unable to exchange relevant information relating to ML and TF with their EU and non EU-counterparts, which complicates cross-border preventative action.

2.5.5 The size of the problem/Baseline scenario

The table in Annex 7 gives an anonymised overview of the current situation in the 16 Member States[28] that have or are in the process of putting in place automated mechanisms that enable them to identify holders of bank and payment accounts.

In principle, an FIU should check the identity of the holders of bank and payment accounts (through a search request) for every STR it receives, or at least be able to do so (see sample table in Annex 7 with total number of STRs per year and per Member State (MS), ranging from 510 to 118.559 STRs). If no such automated mechanisms are available, FIUs should (at least theoretically) gather this information by issuing blanket requests for each STR they receive, resulting in very significant annual administrative costs (both for FIUs and the financial sector). The cost for such blanket requests is illustrated by the sample table in Annex 7 (ranging from approximately. €94 000 to €245 000 000 per year).

Improvements in dealing with the lack of access or delayed access by FIUs to information on the identity of holders of bank and payment accounts may come from more Member States putting in place automated mechanisms at national level allowing for timely access to such information. As a consequence, the traceability of criminal and terrorist financing flows, both nationally and cross border, could also be facilitated and increased. However, it cannot be assumed that uncoordinated action at Member State level would produce sufficient effects, as this depends on the level of commitment across all Member States. Weak spots, that can be exploited by criminals and terrorists to channel their funds in and out the EU financial system, will remain in the EU.

3. EU RIGHT TO ACT AND SUBSIDIARITY

The legal basis of the initiative will be article 114 TFEU.

This initiative aims at providing a harmonised approach to swiftly strengthen the EU's existing framework for the prevention of ML and, in particular, TF on a limited number of identified subjects.

The problems related to the effective detection of criminal and terrorist financing flows have a cross-border dimension. An ineffective AML/CFT framework in one Member State may be exploited by criminals and have consequences on other Member States. It is therefore important to have a harmonised framework at EU level. The FATF is currently also examining what further action can be taken to strengthen the fight against TF. However, this work will take time and even if this leads to a change in the FATF standards (which is not certain), those standards would not be legally binding. Consequently, if the FATF were to modify its standards, these would still need to be translated into EU law and aligned with the existing provisions of the 4AMLD (which in itself constitutes a transposition of the current FATF standards).

As massive flows of illicit money and TF can damage the stability and reputation of the financial sector and threaten the internal market, any measures adopted solely at national level could have adverse effects on the EU Single Market, and result in fragmentation.

This is particularly the case with **virtual currencies** where there is currently no European consistent approach of this phenomenon (see Annex 5). The measures taken by Member

[28]Italy, Spain, Belgium, Bulgaria, Croatia, Greece, France, Czech Republic, Poland, Germany, Lithuania, Portugal, Romania, Slovenia, The Netherlands, Austria.

States are heterogeneous, in their definitions of what virtual currencies are (units of accounts/financial instruments for Germany, scriptural money for Luxemburg, means of payments for Sweden …) as well as in the requirements (authorisation, registration, banking or payment license) which should apply to those providers engaged in VC exchange. This continued trend would lead to regulatory arbitrage. Moreover, some planned measures are not sufficiently addressing the identified problems leaving major market players (such as custodial wallet providers) outside of the regulatory scope.

In the area of **prepaid cards**, the temptation for Member States will be between suppressing all CDD exemptions for prepaid cards, which in some circumstances might give rise to issues of proportionality and necessity, and adopting a varying range of supplementary national measures for prepaid cards to qualify for an exemption. That approach would undermine the Single Market for those instruments.

With regard to **enhanced CDD measures towards high risk third countries**, differences in Member States approaches and practices can lead to gaps and discrepancies in the management of business relationships involving high risk third countries, thus allowing criminals and terrorists to exploit potential loopholes or take advantage of more lenient legislation through regulatory arbitrage, in order to channel their funds in and out the EU.

In the area of **FIUs** it cannot be assumed that uncoordinated action at Member State level would produce sufficient effects, as this depends on the level of commitment across all Member States: (i) the survey conducted under this impact assessment shows that – despite the recommendation formulated in recital 57 of the 4AMLD - not all Member States are planning to put in place centralized registries or mechanisms enabling the identification of holders of bank and payment accounts, and (ii) the clarifications provided by the FATF on the interpretation of the standards regarding the powers of FIUs are currently still not shared by certain Member States.

This is also why Member States, at the JHA Extraordinary Council of 20 November 2015 and at the ECOFIN Councils of 3 December 2015 and 12 February 2016, besides the political message they sent about their unity in the fight against terrorism and terrorist financing, supported the need for action at European level, calling on the Commission to act swiftly. As a result, those Member States[29] that were considering revising their national AML/CFT legislation decided to stop their work and rather wait for the coordinated European response. The European level is seen as the proper one by Member States themselves in terms of effectiveness and efficiency.

Finally, it is also to be highlighted that a strongly integrated EU legislation in the field of AML/CFT will also allow the EU to more effectively contribute to the standard-setting process in the relevant international fora (such as for example in the FATF, MONEYVAL,…).

[29] For instance, the UK.

4. POLICY OBJECTIVES

General objective	prevent ML and TF by more effective detection of criminal and terrorist financing flows

Specific objectives	improve the detection of suspicious transactions coming from or going to high-risk third countries through more legal certainty for obliged entities as regards the ECDD measures which need to be applied protect the financial system of the EU internal market from ML/TF risks through a global EU response to threats posed by high-risk third countries
	improve the detection of suspicious virtual currency transactions and increase the transparency of such transactions by linking them to identities
	reduce the misuse of anonymous prepaid instruments for the purpose of ML/TF
	improve FIUs' access to – and exchange of - information held by obliged entities
	improve swift access by FIUs to relevant information on the identity of holders of bank and payment accounts avoid (i) the use of blanket requests that are costly and delay the collection of such information, or (ii) the non-action of FIUs linked to lack of efficient mechanisms to collect the information

5. POLICY OPTIONS

5.1. Option 1: Maintaining the status quo

See sections regarding the size of the problem/Baseline scenario.

5.2. Option 2: Non-regulatory option

A mapping exercise is currently being conducted within the FIU Platform to identify practical obstacles to access to, exchange and use of information as well as operational cooperation. Consequently, the option of an EU FIU assisting and supporting Member States FIUs was discarded in the current impact assessment, pending the result of this mapping exercise.

In addition to this, the Commission is also conducting a supranational assessment of money laundering and terrorist financing risks (as foreseen under the 4AMLD), which could lead to the formulation of Recommendations to Member States.

The Commission is also deepening its engagement within international fora dealing with counter-terrorist financing in order to enhanced the need for cooperation and exchange of information on this strategic field. In particular, the Commission is closely involved in the implementation of the FATF strategy on combatting terrorist financing.

Regarding prepaid cards, card schemes have the ability to impose through contractual arrangements specific AML/CTF obligations on the prepaid card issuers they work with.

See Annex 9 for more details on the non-regulatory options.

5.3. Option 3: Regulatory options

A regulatory option implies a legislative modification of the existing AML/CFT framework. Legislative options, to address the five specific objectives can be summarised as follows:

5.3.1 Improving the effectiveness of EU policy for high-risk third countries via a harmonised EU approach for enhanced due diligence measures to be applied by obliged entities

5.3.1.1 Option A – to provide a prescriptive list of enhanced customer due diligence measures and require obliged entities to apply at least all of them when dealing with high-risk third countries designated by the Commission

This option will consist in establishing an EU list of ECDD measures that should be applied by obliged entities to enhance the monitoring of financial transactions involving high-risk third countries listed by the Commission.

This list of ECDD measures would rely on the seven measures already provided by FATF recommendations (see point 2.1.1) and already well known by obliged entities and Member States. They will consist in (i) requiring additional information on the customer, (ii) the source of funds, (iii) the intended nature of the business relationship and (iv) the reasons for the intended or performed transaction, together with (v) the approval of senior management to commence or continue the business relationship, (vi) the conducting of enhanced monitoring of the business relationship (such as increasing the number and timing of controls applied, and selecting patterns of transaction that need further examination) and (vii) the requirement that the first payment shall be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In addition, this option would require obliged entities to apply all these ECDD measures to business relationships they conduct with high-risk third countries. The ECDD measures will be considered as a minimum set of requirements imposed by all Member States. Obliged entities and Member States would still be allowed to provide, at national level, complementary ECDD measures, in addition to the minimum set of requirements mentioned above.

5.3.1.2 Option B – to provide a prescriptive list of enhanced customer due diligence measures and an illustrative list of counter-measures, and require obliged entities to apply at least all the ECDD measures and/or, where appropriate, one of the countermeasures when dealing with high-risk third countries designated by the Commission

This option is based on option A combined with a list of counter-measures. In accordance with the FATF recommendations, counter-measures are currently applied to two countries (Iran and North Korea) as they present serious strategic AML/CFT deficiencies (see list of countermeasures in Annex 4).

While the list of ECDD measures would remain mandatory and common to all EU Member States, the list of counter-measures would be presented as illustrative only and mainly bring legal certainty as regards the nature of such counter-measures. These counter-measures would be primarily applicable to high-risk countries identified in FATF recommendations (see point

2.1.1. footnote 7), but could be extended to other countries listed by the Commission where appropriate.

Under this option, obliged entities and Member States will still be allowed to provide, at national level, complementary ECDD measures, in addition to the minimum set of requirements mentioned above.

5.3.1.3 Option C – to provide a prescriptive list of enhanced customer due diligence measures and an illustrative list of counter-measures, and require obliged entities to apply all of the ECDD measures and/or, where appropriate, one of the countermeasures when dealing with high-risk third countries identified at EU, national and sectorial level.

This option is based on option B but would apply not only to the financial transactions involving high-risk third countries listed by the Commission, but also to high-risk third countries identified by the Member States in their national legislation and by obliged entities themselves in the context of their sectorial risk assessments.

Under this option, the abovementioned list of seven ECDD measures will apply to all high-risk third countries identified, whatever the source of this identification.

5.3.1.4 Stakeholder views on the problem and options

Member States were consulted about the opportunity to put in place a harmonised and coordinated EU policy towards high-risk third countries. 23 Member States agreed that there was a need for a minimum degree of harmonisation in this field. Only three Member States disagreed with the approach suggested under options A and B, arguing that it would go against a risk-based approach.

21 organisations were consulted. Some of their members already implement option A, given that they apply the whole range of above-mentioned ECDD measures to all of the high-risk third countries identified by FATF (in particular). For those who do not apply this global approach, option A is recognised as beneficial as it will give clearer guidance on how to manage business relationships with high-risk third countries and will enhance their capabilities to verify the data provided by a customer to detect suspicious activities. From a technical point of view, stakeholders saw it as an improvement for the risk management processes, in particular because the process will be automated and will limit manual checking. A harmonised approach was also viewed as a way to minimise operational and reputational risk and achieve a more consistent interpretation of ECDD obligations, ensuring a level-playing field.

Concerning the implementation of counter-measures, it seems that obliged entities do not properly make use of counter-measures within the meaning of the FATF recommendations. On the basis of the feedback received from the written consultation, while an important number of obliged entities indicate that they apply counter-measures, it appears that only a few of them apply counter-measures falling under the FATF definition (such as limitation of transactions, termination of business relationship etc.). In other cases, so-called "counter-measures" are much more similar to complementary ECDD or only ECDD. Obliged entities see in option B an opportunity to bring legal clarity to the issue.

Some obliged entities expressed concern about cost implications (IT costs) and the potential administrative burden caused by overly prescriptive rules. They insisted on the need to combine the intended coordinated policy with the principle of the risk-based approach.

For this reason, both private sector representatives and Member States were not supportive of option C, which was considered to be excessive and not to reflect the principle of a risk-based approach. While the EU list of high-risk third countries could lawfully trigger the same level of ECDD measures all over the EU, obliged entities consider that their own list of high-risk third countries still benefits from applying a risk-based approach, with appropriate customer due diligence measures depending on the specific national or sectorial contexts.

In the specific case of money value transfers services, only 3 contributions were received and reflected very different views:

- two representatives of the sector indicated that the lack or minimum harmonisation of AML/CFT rules involved managing one-off regulatory requirements which are time-consuming and costly. A greater harmonisation of AML/CFT rules across the EU would also contribute to reducing the risks of misuse by increasing the levels of compliance. A harmonised regime was perceived as improving the ability to limit risk, in particular for activities that are conducted in different jurisdictions. One actor, in particular, indicated that its current ECDD program with high risk countries was already very robust and in line with the Commission's harmonisation plan, and that no major impact was expected.
- one representative of this sector, while recognising that the impact on its business would be very limited, indicated a preference to stick to the risk-based approach, because of the potential risk that disproportionate rules may hamper legitimate remittance flows to high-risk jurisdictions.

When asked about the cost implications of a harmonised approach on ECDD measures, obliged entities were not able to provide concrete information, since they do not include such parameters in their internal auditing systems.

5.3.2 Improving the detection of suspicious virtual currency transactions and increasing the transparency of such transactions by linking them to identified persons

Legislative options to reduce VCs' anonymity could range from light options (such as imposing few requirements on one or various market players in order to lift anonymity at a designated point in time), to a total ban of the activity if considered too high a risk for criminal purposes.

Reducing or lifting VC's anonymity can be done through targeting three players within the virtual currency ecosystem: **users, exchange platforms and custodial wallet providers.** The remaining major stakeholder (so-called 'miners'), are more difficult to reach as most of them are located in China (see discarded options).

The three above options to tackle anonymity will therefore be examined on a stand-alone basis as well as in combination, as several market players can be targeted simultaneously. The objective is to reduce anonymity as much as possible and targeting only one category of players may not be sufficient.

5.3.2.1 Targeting users

Users include consumers and retailers using VCs as an investment product or as a means of exchange for buying/selling products or services. They transact using VC addresses. Their identities are never exchanged online which makes transactions anonymous and opaque to law enforcement authorities.

Option A - lift VCs' anonymity through the mandatory registration of users

Under this option, different levels of anonymity could be envisaged. If registration is mandatory, it could link registration and access to the payments network (for example by making use of Legal Entity Identifiers (LEI) mandatorily for VC transactions).

Option B – reduce VCs' anonymity through the voluntary self-registration of users

This option would offer users a clearly defined voluntary channel to 'self-identify' (e.g. to the national FIU), or some other national or international bodies/registries such as the European Banking Authority). Anonymity in payments could still be upheld (e.g. using public key infrastructures) but authorities combating financial crime could rapidly verify identities of registered users.

5.3.2.2 Targeting exchange platforms

In order to acquire VCs, VC exchange platforms are a major gateway. Requesting exchange platforms to collect identities implies submitting them to one of the two following options.

Option C - lift VCs' anonymity through the regulation of exchange platforms under the 4AMLD

This option would make VC exchange platforms obliged entities under 4AMLD, requesting them to verify the identity of their customers and report suspicious transactions that may involve ML or TF to FIUs.

In practice, the obligations that would fall on exchange platforms under the 4AMLD are the ones described in Article 11 of the 4AMLD which mainly consist in applying CDD measures when establishing a business relationship, when carrying out an occasional transaction above €15 000 or when there is a suspicion of ML or TF regardless of any derogation.

Customer due diligence measures consist in identifying the customer and verifying his identity on the basis of documents, data or information obtained from a reliable and independent source, identifying the beneficial owner, assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship and conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of the relationship.

Option D - lift VCs' anonymity through the regulation of VC exchange platforms under the revised Directive on Payment Services (PSD2)

PSD2 goes further than 4AMLD. On top of the AML/CFT requirements which it automatically imposes, by reference to the 4AMLD, on the entities that fall under its scope, the PSD2 also establishes a licensing obligation for regulated entities, minimum capital requirements, safeguarding requirements, and consumer protection rules.

Submitting exchange platforms to PSD2 would automatically bring exchange platforms under 4AMLD (option C) but would also submit them to broader consumer protection rules, licensing requirements and safeguarding requirements. The VC exchange platforms would be

regulated as any other payment service provider and will gain a higher degree of legitimacy as would the virtual currency market in itself.

Having recourse to PSD2 would (i) require that VC currency exchange platforms comply with many other provisions of PSD2 (licensing, capital requirements, information, etc) which they would need more time to conform to, and (ii) would go beyond the current focus of the IA on strengthening the fight against terrorist financing.

5.3.2.3 Targeting custodial wallet providers

Contrary to software wallet providers (which provide applications or programs running on users' hardware (computer, smartphone, tablet…) to access public information from a distributed ledger and access the network), custodial wallet providers include the custody of the user's public and private key (fully or shared with one or more customers). Compared to traditional financial services, custodial wallet providers are quite similar to financial institutions holding bank or payment accounts.

With a growing network of acceptance, the need to "cash-out" of VCs and exchange them for FCs might decrease with time. This trend would increase further if VCs became less volatile.

Option E - lift VCs' anonymity through the regulation of custodial wallet providers under 4AMLD

Like option C, option E would imply that custodial wallet providers perform CDD and report suspicious transactions.

Option F - lift VCs' anonymity through the regulation of custodial wallet providers under PSD2

Similar to option D, using PSD2 for custodial wallet providers would mean bringing custodial wallet providers automatically under 4AMLD and introducing broader consumer protection rules, safeguarding of funds etc. via their regulation under PSD2.

5.3.2.4 Stakeholder views on the problem and options

While consumers expressed some concern in reducing the anonymity of VCs, they concurred with the need to have 'gate-keepers' that manage the control of users' identities when needed (options C, D, E and F).

All Member States were consulted and 27 supported option C with one exception having a preference for option D. Option E was also envisaged by some Member States even though not presented in the questionnaire. Any option involving PSD2 (Options D and F) would not receive the support of most Member States – they considered that this would give too much legitimacy to VCs and drive consumers to believe VCs are safe and sound products in contrast to the list of risks enumerated in the EBA Opinion[30], which is referred to in Annex 5. The EBA in its Opinion considered that a welcomed first step in regulating the virtual currency sphere would consist in reducing the risks linked to anonymity by bringing VC currency

[30] "EBA Opinion on virtual currencies" – 4 July 2014 – page 21 to page 37. Pro memoria, the Commission was an active observer of the EBA Task-Force on virtual currencies that produced that Opinion.

exchange platforms in the scope of the 4AMLD (equivalent to option C). EBA however also suggests a long term approach that would aim to provide a full regulatory regime for virtual currencies.

Finally, the VC industry was generally favourable to legislation that would primarily give them more legitimacy and, secondly, would help to differentiate between players that make the most concerted efforts to track criminals from *bona-fide* users.

Options A and B were only tested with some relevant stakeholders (i.e. consumers/users, experts), with a preference emerging for option B.

5.3.3 Reducing the misuse of anonymous prepaid instruments by further reducing the exemption regime for anonymous prepaid cards under the 4AMLD

A number of options have been considered to further restrict the exemption regime for anonymous prepaid cards under the 4AMLD. Some of these options are of a legislative nature, others are non-regulatory (e.g. targeted geographical or sectoral restrictions to the use of prepaid cards) and are explained in Annex 9. Some options have been subject to an impact assessment, others have been discarded at an earlier stage and are referred to in Section 7 as well as in Annex 8.The following options have been considered in more detail and their impact assessed in Section 6. These options all have for objective to reduce the current exemption perimeter for prepaid cards, ranging from the total suppression of existing exemptions, to a partial suppression when cards are used online and/or a lowering of the threshold above which CDD has to be conducted. The different options are assessed in terms of effectiveness and efficiency, considering market effects both on the supply side (card issuers, distributors) and the demand side (consumers, notably the unbanked people). Options B and C can be combined.

5.3.3.1 Option A - Suppressing all the existing exemptions of 4AMLD for prepaid instruments (i.e. suppression of Article 12 of the 4AMLD)

All anonymous prepaid cards, reloadable or not, would become subject to CDD (identification and verification of the identity of the cardholder) from the first euro. Identification of the cardholder and registration of their identity would have to be carried out from the outset, either by the distributor or by the issuer upon activation of the card. It should be noted that at least 3 Member States have already chosen this option under the 3AMLD and that 6 or 7 Member States are envisaging it in the context of the implementation of the 4AMLD into national law.

5.3.3.2 Option B - Eliminating anonymity for the online use of prepaid cards (reloadable or not)

Under this option, the current €250 threshold for use of prepaid cards in face-to-face situations would remain as it is under the 4AMLD. However, there would be no threshold for the online use of those cards.

This option leaves the current exemption of Article 12 of the 4AMLD unchanged as far as prepaid cards are used in face-to-face situations. In non face-to-face environments (where cash cannot be used), prepaid cards would only be able to be used after the cardholder had been subject to appropriate CDD measures (i.e. verified identification).

This option is less stringent than option A as it limits the suppression of the card exemption to the sole online use of the prepaid card. The view is that cardholders would be more inclined to go through a CDD process online as this would be lumped up with the activation of the card for online use. CDD can be conducted at a distance by the card issuers with the assistance of CDD service providers which would scan online the ID document presented by a cardholder and having its authenticity verified against different databases, and then verify the address by cross-checking data with bank account , phone or mobile number information. This is also a sector which FinTechs are investing in, including in trying to leverage the e-IDAS regulation[31]. Within the next 3 to 5 years, the cost of performing CDD at a distance is likely to drop significantly, as that market develops.

5.3.3.3 Option C - Minimising anonymity by lowering the €250 thresholds both for reloadable and non-reloadable prepaid cards

Markets have not made full use of the €250 threshold for non-reloadable prepaid cards, as most cards of that type sold in retail stores carry values ranging from 10, 20, 50 to 100/150 euros (or £100). This option would propose halving the current threshold in the 4AMLD (to €125) or a return to the initial threshold of the 3AMLD (€150).

This option will have no immediate effect for non-reloadable cards as the market offer is in its majority already below this threshold. It will however have a long term in possibly reducing that market segment under normal inflation conditions. This option will however directly affect reloadable prepaid cards as CDD requirements will cut in at an earlier stage of use of the card.

5.3.3.4 Option D - Minimising anonymity by applying simplified customer due diligence from the 1st euro and verifying identity at a later stage, e.g. upon the crossing of a threshold, e.g. €250

Under this Option, simplified CDD would be applied at the time of the purchase of the prepaid card. The buyer would be required to show an ID document (as, for example, is the case for the purchase of tobacco or alcohol to avoid minors having access to such products). The formal verification of the buyer's identity would take place at a later stage, e.g. after some usage of the card, or upon the crossing of a threshold. This option, based on a suggestion from industry is inspired by the simplified due diligence approach foreseen under Article 15 of the 4AMLD. However, its blanket application to all anonymous prepaid cards would raise questions of proportionality and effectiveness.

5.3.3.5 Option E – Lowering the thresholds under the 4AMLD for non-reloadable cards and requesting the application of CDD (simultaneous identification and verification of identity) for reloadable cards from the first euro

Contrary to Option B where the emphasis is put on the use of the card (offline vs. online), under this option, the requirements vary according to the nature of the card. This option consists in lowering the existing threshold for non-reloadable cards from €250 to €150, and in suppressing the current threshold for reloadable cards, which are the closest proxy to a debit

[31] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

card or a credit card (which are currently already subject to CDD) and for which there is some logic in applying similar CDD requirements in terms both of timing and intensity.

5.3.3.6 Stakeholder views on the problem and options

Member States were fairly divided on the various options available. About half of the Member States supported a mandatory online identification when activating a prepaid card. There was no fixed view on the thresholds to apply for CDD for both reloadable and non-reloadable prepaid instruments.

Consumer organisations were of the view that a decision on these matters was the responsibility of public authorities. They nevertheless expressed the need to preserve the financial inclusion dimension offered by prepaid cards. They therefore expressed a preference for the options that would present value in limiting risks whilst allowing for continued provision of services to the unbanked.

Industry was not in favour of any change in legislation, considering that the 4AMLD still to be transposed into national law is much stricter than the 3AMLD in respect of general purpose reloadable cards. The main concerns for card issuers is to perform CDD as late as possible in the lifetime of a prepaid card, or at least not before the cardholder has had time to appreciate the instrument, is therefore likely to use it repeatedly, and even to upgrade the card in its functionalities (moving for instance from a non-reloadable card to a reloadable card). This repeated use of the card in many business models is a source of revenue generation which will make the absorption of CDD costs easier for card issuers. This approach, of course, creates an inherent tension with a public policy whose goal is to lift or reduce anonymity as soon as possible and hence to have CDD being performed as early as possible.

Prepaid card issuers are of the view that **Option A** might eliminate non-reloadable prepaid cards from the market or at least their distribution via the retail channels (supermarkets, newsagents, tobacconists), as these products are low value, low margin ones and could with difficulty absorb CDD costs. As a matter of fact, the non-reloadable prepaid segment is regulatory driven, because issuers prefer to eschew CDD and only sell prepaid cards with nominal values below threshold. Consumers are concerned that the unbanked part of a population might be deprived of a useful payment tool that gives them access to e-commerce and cheaper products and services. This concern is at least partly mitigated by the Payment Account Directive which foresees that any person lawfully residing in the EU can have access to a basic bank account equipped with a debit card.

Option B is a less stringent variation of Option A. It better takes into account the wish of consumer organisations that the unbanked continue to have access to general purpose prepaid instruments, as the online performance of CDD will not affect distribution channels and notably retail distribution. Card issuers, notably those who may have a range of products concentrated on the low value non-reloadable cards, are likely to continue challenging the suppression of the CDD exemption for the online use of such cards, as it will mean that they will have to absorb CDD costs upfront, unless they charge an upfront fee to the cardholder[32].

Following discussions with market players with regard to **Option C**, it appeared that the AML/CFT legislation through the setting of CDD exemption thresholds shaped the market for non-reloadable cards. In practice, no such cards can be found in the market with a value in

[32]The Belgian post office prepaid card scheme requires a yearly annual fee of 12 euro for its reloadable prepaid card, no fee for online reloading via a credit transfer (which requires a payment/bank account) but €3.50 if reloaded at the counter, and €4 for each ATM withdrawal.

excess of €250. More surprisingly, the core market for non-reloadable cards is represented by cards with values ranging from €25 to €150 (or up to £100).

The lowering of the current AML/CFT threshold, for instance from €250 to €125 or €150, would therefore leave prepaid card issuers unaffected, as market needs for non-reloadable cards could still be served without having to perform CDD (and consequently having to support related costs). Re-aligning the 4AMLD threshold for non-reloadable prepaid cards on that of the original 3AMLD (i.e. €150) will have no effect on today's market but will bite in the future in an inflationary context.

The main impact therefore concerns reloadable general purpose prepaid cards, which are the closest means of payment to a debit card linked to a payment account (the latter is regulated under today's AML/CFT requirements subject to a full CDD).

Option D is the one favoured by industry. Its additional requirements are only marginal compared to those defined by the current 4AMLD.

Option E is a less stringent alternative to Option B. It is therefore more palatable to industry than Option B as reloadable cards are – by definition - more likely than non-reloadable cards to be used many times and therefore offer better prospects in terms of CDD cost absorption.

5.3.4 Improving FIUs' access to – and the exchange of – information held by obliged entities

5.3.4.1 Option A – aligning EU law with the latest international standards on AML/CFT in this field and clarifying FIU powers

Under this option, the 4AMLD would be amended to clarify that an FIU shall obtain available information from any obliged entity in the event of a suspicion relating to ML/TF, even if this obliged entity did not previously report an STR. Such an approach is in line with international standards and the interpretation on the methodology agreed by FATF in October 2015.[33] It follows that this approach shall also be applied when an FIU receives a request from another FIU to obtain additional information from an obliged entity.

Similarly, the 4AMLD would be clarified by ensuring that obliged entities should provide all necessary information **directly** to the FIU at its request.[34] This is also consistent with the 4AMLD provisions on the operational independence and autonomy of FIUs. Obtaining information from obliged entities is part of the core business of their analysis function – and hence would be considered as a task to be performed directly by an autonomous FIU.

5.3.4.2 Option B: Establishing a single European FIU to receive, analyse and disseminate results to national competent authorities

Under this option, the EU would establish a single European FIU to receive, analyse and disseminate to the competent authorities disclosures of information from obliged entities operating within the EU. Such an option was already considered in the impact assessment

[33] See criterion.29.3 in the FATF methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems: "In the context of its analysis function, an FIU should be able to obtain from any reporting entity additional information relating to a suspicion of ML/TF. This does not include indiscriminate requests for information to reporting entities in the context of the FIU's analysis (e.g., "fishing expeditions")."

[34] See the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, COM(2013) 45, article 32(1)(b).

accompanying the 4AMLD[35]. Obliged entities would be required to provide directly all the necessary information at the request of the single European FIU which would disseminate the results of its analysis to the national competent authority. In the event of a suspicion of ML/TF, the single European FIU would be empowered to obtain additional information held by any obliged entity in the EU, even if this obliged entity did not previously report an STR.

Where Option A aims at reaching the general and specific objectives through a clarification of the existing EU legislation/structures, Option B aims at reaching the same objective in a much broader way, through an institutional reform of the FIU function at EU level.

5.3.4.3 Stakeholder views on the problem and options

For Option A, stakeholders were generally strongly supportive. Following the adoption by FATF of the interpretation regarding criterion 29.3 (cf. text in footnote), there is an international consensus that FIUs should be able to obtain additional information from any obliged entity in the event of a suspicion of ML/TF. The EU FIU platform was consulted and all replying FIUs supported the interpretation of FATF. The overwhelming majority of FIUs (23) therefore supported a codification of this interpretation by amending the 4AMLD, while two FIUs abstained at this stage from replying. One police FIU noted that the FIU function may move towards an investigatory power, rather than for intelligence work or FIU analysis, which may lead to operational and resource issues.[36] With regard to direct access to information held by obliged entities, unanimous support was offered by FIUs (25 FIUs responded in total), who felt that FIUs should have such power.[37]

Member States equally demonstrated significant support for this approach. They tended to agree that FIUs should have direct access to information held by obliged entities, even if those obliged entities did not report an STR[38].

Option B was discussed in the past in the context of the EU FIU platform and in the Impact Assessment of the 4AMLD. This approach does not benefit from much support currently. The option remains very sensitive since it implies both a substantial transfer of sovereignty and a deep adaptation of national systems. Member States would prefer a more tailor-made approach of cooperation between national and EU levels. Instead of a single EU FIU, some Member States would be more open towards an EU FIU assisting and supporting Member States' FIUs. This option has been discarded for the purpose of this impact assessment since the Commission announced that it will be covered under another initiative of the Action Plan on Terrorist Financing (see Annex 8).

5.3.5 Providing FIUs (and potentially other AML/CFT competent authorities) with an efficient mechanism to ensure timely access to information on the identity of holders of bank and payment accounts

[35] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013SC0022

[36] The Commission clarified that the scope of the 4AMLD only covers the FIUs' role of analysis and is not covering investigation phase to be carried out by law enforcement.

[37] In this context, 2 FIUs expressed that this task should be carried out according to the procedures established by the applicable legislation while all the other ones preferred to remove any ambiguous wording in this regard.

[38] One Member State nevertheless expressed some cautious regarding direct access by the FIU to information held by obliged entities. This is due to the fact that the police, as leading investigation authority, has the power to obtain financial information based on a court order only. Giving more powers to the FIU (in contrast to law enforcement) could induce some operational challenges for this Member State.

The options need to address the main problems related to FIUs' access to such information - (i) the fragmentation of information, (ii) the lack of swift access by FIUs to this information and, (iii) the costs and delays related to the issuance of unnecessary blanket requests to the financial sector (or non-action) by FIUs.

Furthermore, information that will be available to FIUs should be reliable (i.e. unbiased) and limited to what is necessary to achieve the objective (proportionality) and handled with the necessary safeguards. The minimum information that should be available through the mechanism in order to fulfil the objective is set out in Annex 7.

5.3.5.1 Option A – an automated central registry at Member State level, directly accessible to national FIUs (and other national AML/CFT competent authorities) for AML/CFT purposes

The first option could consist in requiring Member States to set up an automated central registry at national level, containing the necessary data allowing for the identification of holders of bank and payment accounts, and granting their own national FIUs (and potentially other national AML/CFT competent authorities) direct access, under defined conditions, to the information kept in the registry.

Under this option, Member States would have to define the type of information needed to feed into the registry, and require financial institutions to upload this information periodically into the database of the registry ("input phase").[39] Member States would also have to define the technical and legal conditions for access to this registry by FIUs or other AML/CFT competent authorities ("consultation phase").

Currently, eleven Member States have (or will soon have) automated central registries in place allowing for the identification of holders of bank and payment accounts. Nine Member States allow (or will allow) FIUs to have access to the information in these registries.

Example 10: The Belgian banking registry, currently only available to tax authorities for tax purposes

Taking into account the National Bank of Belgium's expertise in the secure management of large quantities of data, it was entrusted with the task of establishing and managing, on behalf of the Federal Public Finance Service the Central Contact Point for account numbers. To this end, it keeps a central registry containing - amongst others - the account numbers of 46 million bank accounts held in Belgium by 17 million resident and non-resident natural and legal persons. The information has to be supplied by credit institutions, payment institutions, investment firms, etc. Their declarations never state the amounts relating to the accounts listed. Identification of natural persons occurs through the National Identification Number, or through a limited set of personal data (name, date and place of birth). For EU accounts, the identification of the account number can only be done by using the International Bank Account Number (i.e. "IBAN code", available in all EU Member States).

Consultation is secure and is restricted to persons authorised by the tax authority following a procedure which is strictly defined by law (indirect access, through a prior request filed with the Central Contact Point). The natural and legal persons holding the accounts may also exercise their right of consultation free of charge, and if necessary request correction or deletion of incorrect data by their financial institution.

Source: The National Bank of Belgium Corporate Report 2014, p. 15-16, www.nbb.be and the Royal Decree of 17 July 2013, appointing the National Bank of Belgium as Central Contact Point, modified by the Royal Decree of 3 April 2015.

5.3.5.2 Option B – an automated central mechanism at Member State level, directly accessible to national FIUs (and other national AML/CFT competent authorities) for AML/CFT purposes

[39] In practice, such uploading can be done through an IT protocol.

The second option could consist in requiring Member States to set up an automated centralised mechanism, thus leaving the choice for the IT architecture to be used for reaching the objective to the discretion of Member States. Consequently, Option B also fully includes Option A, as such automated centralised mechanisms could take various forms, ranging from a central registry (option A) to a central automated data retrieval system (e.g. a single IT portal, retrieving the information from different underlying (existing) databases).

Under this option, Member States would also have to define the type of information that has to be accessible through this mechanism, and require financial institutions to make this information available under the mechanism ("input phase"). Finally, Member States would also have to define the technical and legal conditions for direct access to the mechanism by FIUs or other AML/CFT competent authorities ("consultation phase").

Currently, three Member States have a central data retrieval system/electronic information system in place, or are in the process of setting them up.

Example 11: The German automated central data retrieval system, which is accessible - via the German financial supervisor ("BaFin") - to a broad range of authorities

On 1 April 2003, official online access to account details was introduced in Germany. Pursuant to the German law, every credit institution is obliged to maintain a separate and up-to-date file containing details of all bank accounts and safe custody accounts held by its clients in Germany. This file must include specific master data related to the customer, their proxy holders, and, if applicable, other economic beneficiaries. These files do not contain information on balances or account transactions. The German financial supervisor, BaFin, is empowered to retrieve this data at any time. On the retrieval system, BaFin's annual reports of 2002 and 2003 highlighted the following:

"Online access represents a new tool to identify the flow of funds, particularly when it comes to money laundering and the financing of terrorism. (...) The particularly time-consuming process of requesting information from around 2,500 credit institutions is a thing of the past.
(...)
Seven weeks after its launch, regulators processed about 2,200 inquiries including just under 1,600 inquiries directed to BaFin by prosecutors and the police. 425 inquiries came from BaFin itself, mainly relating to cases of unauthorised financial transfer transactions. BaFin was able to provide information on a total of more than 9,600 accounts in response to internal and external inquiries. To obtain this information, BaFin accessed the data of participating credit institutions about 5.5 million times. In several instances, and with the help of account information from BaFin, investigating officials were able to seize previously unknown assets of persons charged. It was also possible to determine quickly whether or not suspected terrorist organisations had accounts in Germany."

In its annual report of 2011, BaFin reiterated the importance of the retrieval system - and the quality of the information it contains - in the fight against ML and other forms of crime:

"The success of the account information access procedure – an elementary tool in the pursuit of money laundering, other criminal offences and unauthorised business transactions – depends crucially on the accuracy of the data stored."

Source: BaFin's annual report 2002, p.18, report 2003, p.69, and report 2011, p. 252.

5.3.5.3 Option C – an automated central registry or mechanism at Member State level, directly accessible to a broader range of national authorities and for a broader purpose

A third option could consist of requiring Member States to put in place central registries or central automated mechanisms allowing for the identification of holders of bank and payment accounts, and make this information accessible to a broader group of national authorities (FIUs, tax authorities, police, customs etc…) and for a broader enforcement purpose than the mere prevention of ML and TF. Consequently, Option C would entirely encompass Option B.

As far as the "input phase" is concerned, this option is equal to options A and B. The difference with options A and B lies in the "consultation phase", as the registry or mechanism would be directly accessible to a broader range of authorities for a broader purpose, including

law enforcement and judicial authorities, thus harmonizing at EU level the use of such registry or mechanism to fight all types of crime in general, and identify proceeds of such crimes in view of recovery (freezing and confiscation).

Currently at least twelve Member States have automated central registries or mechanisms in place that are accessible to a broader range of authorities for a broader purpose.

5.3.5.4 Stakeholder views on the problem and options

The Commission received replies from 25 FIUs (main stakeholders) to its consultation. 24 FIUs were in favour of putting in place a registry/efficient mechanism allowing FIUs to swiftly identify holders of bank and payment accounts in all Member States. One FIU expressed no position.

The consultation highlighted the lack of swift access to information on the identity of holders of bank and payment accounts – either by FIUs themselves or for other EU FIUs – as a two-fold problem: (i) FIUs complained that counterparts lacking access are unable to reply to their requests for a cross-border exchange of information within the EU, and (ii) they highlighted that without this information they are unable to exercise their own powers to block or suspend suspicious financial transactions swiftly. One FIU pointed out that the lack of overview of all accounts belonging to a suspect leads to "partial (freezing) actions" which alert the suspect, who is then able to remove the remaining undetected funds from the other accounts.

As far as the consultation of the financial sector is concerned, only a few replies were received, coming from institutions situated in three Member States. They raised: the importance of data protection and proportionality (data should only be accessible for public authorities, not to other banks), a clear definition of the scope (necessary data, type of accounts, frequency for the updating etc.) and the costs linked to the filing/uploading of the information. Two financial institutions highlighted that a registry/mechanism would have a positive impact on the security of financial institutions and the EU financial system/would minimise the number of (irrelevant) requests for information from authorities. Finally, one large banking group, active in different Member States[40], stated that a great number of European countries have such registries/mechanisms in place already, and therefore it would be useful to harmonise the information to be filed/uploaded in the different countries, allowing financial institutions to establish a uniform technical process.

In January 2016, Europol wrote to the Commission stressing the importance of centralised bank account registers for law enforcement in the EU, stating that such registers are vital to swiftly trace, identify and freeze criminal assets, and to follow suspicious financial flows relating to ML, TF and corruption. In this respect, Europol is in favour of wider access (than mere FIU access) to such registries by the law enforcement community. On 3 March 2016, Europol transmitted a report to the Commission which was drafted by the subgroup of the Asset Recovery Offices Platform on the establishment of centralised bank account registries at national level. This report describes the current situation across Member States and formulates a set of recommendations (cf. Annex 7), including the setting up of national centralised bank account registries in all Member States.

[40] The group gave replies for its EU establishments situated in Germany, France, Italy, Belgium, Malta, Portugal, Austria, Greece, Spain, Czech Republic, Poland, Hungary and Luxemburg.

6. ANALYSIS OF THE IMPACT OF THE POLICY OPTIONS PROPOSED

6.1. Option 1: Maintaining the status quo

See section 2 – problem definition.

6.2. Option 2: Non regulatory option

Some of the non-regulatory option might marginally improve the situation with regard to the baseline scenario, but they will not adequately address the specific and general objectives. Furthermore, the mapping exercise and the supranational risk assessment still deserve more in depth analysis, and will therfore not allow for a swift improvement of the AML/CFT framework.

As regards the powers of FIUs, the consultation process has highlighted that – despite the clarifications provided by the FATF regarding the interpretation of the standards in this area – some Member States indicated that they have a different understanding of the current EU provisions, hence the need for a regulatory action in this field.

See Annex 9 for more information on the impacts of the non-regulatory options.

6.3. Option 3: Regulatory options

Preliminary remark: as the proposals concern five limited and targeted modifications to the recently adopted 4AMLD, this impact assessment builds upon the impact assessment of the 4AMLD for the general aspects (such as data protection and fundamental rights, impacts on SME's, consumers, etc…), and therefore only highlights additional impacts that could be generated by the proposed targeted amendments. This is also particularly the case a far as the quantification of costs and administrative burden linked to AML/CFT is concerned, where reference is made to p 43-50 of document SWD(2013) 21 final. The current impact assessment therefore solely focusses on the (limited) additional costs and administrative burden that could be generated by the five proposed modifications.

6.3.1 Improving the effectiveness of EU policy for high-risk third countries via a harmonised EU approach for enhanced due diligence measures to be applied by obliged entities

6.3.1.1 Option A - to provide a prescriptive list of enhanced customer due diligence measures and require obliged entities to apply at least all of them when dealing with high-risk third countries designated by the Commission

Effectiveness

This option would reach the objective of enhanced detection of suspicious transactions relating to high-risk third countries as it would bring more legal certainty to obliged entities through the prescriptive list of ECDD measures and the mandatory application of all of them as a basic requirement.

This option would impose on all Member States the same level of requirements as regards their dealings with countries listed by the Commission and would ensure a more consistent

approach, limiting the risk of regulatory arbitrage and loopholes that may stem from gaps/differences between different sets of national legislation. This approach would allow for comprehensive and harmonised checks and monitoring for all parts of the transaction chain (customer, purpose and nature of the business relationship, source of funds …). In addition, through the systematic approval of senior management, the processing of the financial transaction will benefit from higher scrutiny.

This option would harmonise the requirements as regards high-risk third countries listed by the Commission, making the protection of the EU financial system against ML/TF risks more effective.

Other impacts

Option A is proportionate as it requires the application of already known requirements with no extra burden linked to potential additional rules. It allows for better harmonisation among obliged entities and limits the risk of gaps stemming from different requirements depending on the national legislation concerned.

No adverse impacts are expected from a data protection or fundamental rights perspective as Chapter V of the 4AMLD already fully applies in the context of the option proposed.

Exposure to high-risk third countries

Obliged entities have indicated that their business exposure to high-risk third countries is low and even negligible.

Risk based approach

As mentioned under section 2, the fact to impose specific measures to tackle high risk situations is not in contradiction with the risk based approach, as it concerns the implementation of ECDD to business relationships involving high risk third countries considered as presenting a risk to the EU as a whole.

Costs

Obliged entities were unable to provide specific data on the costs they face today relating to managing their dealings with high-risk third countries. As such, concrete estimates are difficult to provide.

However, other kind of information provided by the industry through questionnaires or bilateral technical meetings brought interesting elements concerning the technical implementation of such ECDD measures, such as the drawing up of questionnaires and templates for the customer, training of staff, IT processes to include "filters" in the customers database etc…

For obliged entities that currently do not apply all of the ECDD measures, this new requirement would imply some administrative and potentially IT costs to supplement their existing ECDD measures (e.g. new questionnaire templates, new IT filters in the transactions process, internal process to obtain senior management approval).

One can assume that the major part of ECDD measures to be put in place mainly require the implementation of standardised procedures (questionnaires, filters including all the designated high-risk third countries to trigger red flags). This systematic and automated check will limit the burden linked to manual checks which are currently undertaken. It would, however, also include a systematic approval from senior management, requiring a judgment-based assessment that may delay the processing of the transaction or commencement of the business relationship (from hours to days depending on the organisation concerned).

6.3.1.2 Option B – to provide a prescriptive list of enhanced customer due diligence measures and an illustrative list of counter-measures, and require obliged entities to apply at least all the ECDD measures and/or where appropriate one of the counter-measures when dealing with high-risk third countries designated by the Commission

Effectiveness

This option would fulfil the objective of enhanced detection of suspicious transactions relating to high-risk third countries, since it would include a reference to counter-measures. Although these counter-measures are limited to countries or jurisdictions with such serious strategic deficiencies that the FATF already calls on its members to apply counter-measures, an explicit reference in EU law would bring more clarity as to what is expected of obliged entities. Obliged entities would benefit from clearer guidance on whether and how ECDD measures or counter-measures apply.

The EU's policy towards high-risk third countries would be stronger and more complete to better prevent the misuse of the EU's financial system.

Other impacts

Option B is equal to option A as regards other impacts.

Exposure to high-risk third countries

As for option A, the business exposure of obliged entities to high-risk third countries is very limited. Moreover, FATF's call for counter-measures is focused on high-risk third countries with serious deficiencies and with whom no contacts, action plans or diplomatic initiatives are conceivable. Currently, the number of such countries is very limited, and it is likely that this number will not increase in the near future.

Risk based approach

Similarly to option A, the fact to impose specific measures to tackle high risk situations is not in contradiction with the risk based approach, as it concerns the implementation of ECDD to business relationships involving high risk third countries considered as presenting a risk to the EU as a whole. While imposing a specific list of ECDD measures is needed to give coherence to this option, keeping the list of counter-measures as an illustrative one is needed to leave obliged entities enough flexibility to choose the most appropriate counter-measures, which are more restrictive than ECDD measures.

Costs

As for option A, obliged entities were unable to provide specific data on the costs they face today relating to managing their dealings with high-risk third countries.

The assumptions developed under option A are likely to be relevant for option B, even with the additional legal requirements related to counter-measures. The nature of possible countermeasures is much more varied than for ECDD measures (e.g. application of specific elements of enhanced due diligence or reporting mechanisms; refusing the establishment of subsidiaries or branches of financial institutions from the country concerned; limiting business

relationships or financial transactions with the identified country etc.). However, it is often the practice among obliged entities not to enter into a business relationship, or to terminate any existing business relationship, with customers from high-risk third countries that are submitted to a FATF call for counter-measures.

6.3.1.3 Option C – to provide a prescriptive list of enhanced customer due diligence measures and an illustrative list of counter-measures, and require obliged entities to apply all the ECDD and/or where appropriate one of the counter-measures when dealing with high-risk third countries designated at EU, national and sectorial levels

Effectiveness

This option would be the most efficient to reach the general and specific objectives, given that the number of high-risk third countries at stake will be higher, i.e. including those identified at national and sectorial levels. Under this option, all these designated countries shall be subject to the same level of ECDD measures with no possibility to apply a risk-based approach according to different national legislation. The detection of suspicious transactions relating to high-risk third countries will be more accurate and complete from an EU point of view.

Other impacts

The new framework that would result from option C could result in overly prescriptive rules that may, in the end, be in contradiction with the overarching AML/CFT principle of a "risk-based approach" which is supposed to allow flexibility to Member States and obliged entities in the choice of the mitigation measures to put in place to address ML/TF risks. While it is legitimate to limit this risk-based approach to address ML/TF risks considered as common to the whole EU (in the context of the Commission's list of high-risk third countries), it seems more proportionate that this flexibility continues to prevail when dealing with countries listed by obliged entities and Member States (according to their national or sectorial specificities).

No adverse impacts are expected from a data protection or fundamental rights perspective as Chapter V of the 4AMLD already fully applies in the context of the option proposed.

Risk based approach

Under this option, the new framework would be overly prescriptive and will be in contradiction with the risk based approach. While it is legitimate to limit this risk based approach to address ML/TF risks considered as common to the whole EU (in the context of the Commission's list of high risk third countries), this flexibility should continue to prevail when dealing with countries listed by obliged entities and Member States (according to their national or sectorial specificities).

Costs

As for options A and B, obliged entities were unable to provide specific data on the costs they face today relating to managing their dealings with high-risk third countries.

While this option is more efficient to reach the objectives, it will nevertheless also be more costly. Indeed, imposing a systematic and mandatory set of ECDD requirements to all designated high-risk third countries, independent of their source, would imply to replicate the

costs potentially at 3 levels (given that the lists of countries may differ depending on the EU, national or sectorial level) and would potentially have an important impact in terms of IT, monitoring and supervision costs.

Exposure to high-risk third countries

The number of affected third countries would be determined through risk assessments conducted at EU, national and sectorial level. The exposure is therefore neither quantifiable nor foreseeable. However, by definition, this scope will be broader than under Options A and B.

6.3.1.4 Comparison of options[41]

Objectives / impacts	Baseline scenario (status quo)	Non regulatory option	Option A Mandatory set of ECDD measures to apply when dealing with high-risk third countries designated by the Commission	Option B Mandatory set of ECDD measures and illustrative list of counter-measures to apply when dealing with high-risk third countries designated by the Commission	Option C Mandatory set of ECDD measures and illustrative list of counter-measures to apply to high-risk third countries designated by the Commission, the Member States and the obliged entities	Comments
Effectiveness regarding the general and specific objectives. **Specific objective:** • Improve the detection of suspicious transactions relating to high-risk third countries and • the protection of the financial system of the EU from ML/TF risks through a global EU response to threats posed by those countries	0	0	++	+++	++++	The Baseline scenario and the non-regulatory option have been identified as not effective to reach the general and specific objective. Option A reaches the general and specific objectives as it will bring more legal certainty to obliged entities on the extent of their AML/CFT requirements to improve the detection of suspicious transactions and it will ensure better protection of the Internal Market, limiting regulatory arbitrage and the risk of loopholes that may stem from gaps/differences in national legislation. Option B will broaden the tools available to detect suspicious transactions by including a reference to counter-measures that may be used against high-risk third countries with serious strategic deficiencies. The protection of the Internal Market against ML/TF risks will be strengthened accordingly. Option C is the most complete mechanism to achieve the general and specific objectives as it will broaden the scope of high-risk third countries considered, i.e. including those identified at national and sectorial levels. All these countries will have to be monitored in the same way with no flexibility granted for obliged entities (potentially departing from a risk-based approach).

[41] In the comparison of options tables the results of the assessment above are compared, with the Baseline scenario representing the status quo set at "0".

Cost-efficiency	0	0	-	-	- - - -	Option A: Concrete estimates are not available. For those obliged entities that do not already implement the full range of ECDD measures, we can assume that this option will trigger limited IT investments considering the nature of ECDD measures at stake (questionnaires, new filters) and possible new administrative constraints (in particular for systematic approval by senior management). At the same time, this automated and systematic check will limit manual checks which are much more cumbersome. In addition, the business exposure to high-risk third countries is very limited. Option B: Concrete estimates are not available. However, the assumptions developed under option A are also relevant for option B. The additional regulatory requirements related to counter-measures are likely to have minor impacts as obliged entities currently have few/no business relationships with high-risk third countries submitted to the FATF call for countermeasures. Option C: Concrete estimates are not available. However, the extension of a mandatory set of ECDD requirements to all designated high-risk third countries will likely trigger new IT, administrative and supervision costs, considering the number of countries considered. If the IT and administrative costs are too high, this may impact the effectiveness of the measure.
Proportionality	0	0	+++	++	- - - -	Option A and B are equally proportionate as they require the same level of requirements throughout the EU for high-risk third countries listed by the Commission. They allow a level-playing field among obliged entities and limit the risk of gaps between national requirements as regards the countries identified in the Commission's list. Option C: The new framework that would result from option C will be overly prescriptive and will be in contradiction with the overarching AML/CFT principle of a "risk-based approach" which is supposed to allow flexibility to Member States and obliged entities in the choice of the mitigation measures to put in place to address ML/TF risks. While it is legitimate to limit this risk-based approach to address ML/TF risks considered as common to the whole EU (in the context of the Commission's list of high-risk third countries), this flexibility should continue to prevail when dealing with countries listed by obliged entities and Member States (according to their national or sectorial specificities).

Data protection/ Fundamental rights	0	0	0	0	-	Any measure resulting in an increased amount of scrutiny leads to a negative impact on privacy and data protection. However, such increased scrutiny is also necessary to reach the objectives. The degree of such negative impact will increase when the scope of the ECDD requirements and/or counter-measures increases, but only in terms of the obligatory measures applied (Option A and B) and/or the potential transactions subject to such measures (Option C). In this respect, Option A and B have a lesser impact that Option C. Option C would also appear more difficult to justify as being strictly necessary from a fundamental rights perspective. It is worth highlighting that the existing Chapter V of the 4AMLD that defines data protection and retention of personal data safeguards framing the use of personal data for AML/CFT purposes fully applies in the context of the options proposed.
Conclusion	0	0	++	+++	- -	Option B is the preferred option as it allows the EU to fulfil its objectives while minimising the impact on cost and proportionality.

6.3.2 Improving the detection of suspicious VC transactions and increase the transparency of such transactions by linking them to identities

Three options targeting respectively users, virtual currency exchange platforms and custodial wallet providers are considered below on a stand-alone basis. However, the recapitulative table presented thereafter allows for a rapid synoptic assessment of their combined effect, as it appears that actions on those three fronts would bring the best results in terms of effectiveness and efficiency.

6.3.2.1 Targeting users

6.3.2.1.1 Option A - lift VCs' anonymity through the mandatory registration of users

Effectiveness

This option would reach the objective of identifying users. By regulating users and submitting them to some sort of obligatory registration, anonymity vis-à-vis the relevant authorities would be lifted. However, the efficiency of such solutions can be called into question considering the difficulties of enforcing such an option. There is no mechanism in place that would ensure that users are registered, since access to virtual currency networks can be achieved through software that does not check any official registration of users.

Costs

The creation of any database generates two types of costs: one-off costs to set up the registry, and recurring costs for the use/maintenance of the tool that national authorities or central authorities would assume. The least costly option would be to have a central database – eg. hosted by EBA instead of 28 national ones – but any database should pose a limited cost as it needs to store only two specific data fields (identity of a user and VC addresses; see calculation below).

This option would not entail much additional cost for users (a simple registration at one point in time on a website).

For VC providers, a mandatory registration would mean asking users for an official identification, which is a marginal cost.

Based on market prices[42], the costs would be estimated as such:

Database (Software)	€28 000
Database Maintenance	€19 000 /year
Operating System Support including securitisation	€6 000
Annual cost of a centralised database year 1	**€53 000**
Annual cost of a centralised database as of year 2	**€19 000**

[42] http://flashdba.com/2013/09/10/the-real-cost-of-enterprise-database-software/

6.3.2.1.2 Option B - reduce VCs' anonymity through the voluntary self-regulation of users

Effectiveness

By offering users a clearly defined, close to costless and voluntary channel to self-identify, anonymity in payments would still be partially upheld. However, authorities combating financial crime could rapidly discard registered users in order to concentrate on unregistered addresses that do not appear in their databases. In this way, self-declaration could serve as a powerful pre-selection device as criminals will typically choose not to identify. As a result, even with an explicitly voluntary element, this could be a highly effective option. This option would also encourage innovation in technologies related to public key infrastructures, permissioned distributed ledgers, privacy by design, etc.

Costs

Identical to option A.

6.3.2.1.3 Comparison of options regarding users

Objectives / impacts	Option A Mandatory registration of users	Option B Voluntary registration of users
Efficiency regarding the general and specific objectives	+++	++
Cost	-	-
Data protection / fundamental rights	0	0
Proportionality	-	+
Conclusion	+	++

6.3.2.2 Targeting exchange platforms

6.3.2.2.1 Option C - lift VCs' anonymity through the regulation of VC exchange platforms under 4AMLD

Effectiveness

Bringing exchange platforms under the regulatory remit of 4AMLD would have the advantage of reaching the objective in an effective and efficient way as: (i) the population of exchange platforms is limited, (ii) a large part of the market would still be covered, and (iii) this option can be put in place very quickly.

Exchanges of VCs into FCs and *vice versa* are the point in time where most of the risks may materialise today with the entry of virtual currencies into the real economy. Global-scale enforcement would be facilitated under this option as this approach has already been advocated by a number of international bodies, including FATF.

Costs

Following discussions with industry actors that already fulfil CDD requirements, the cost of such CDD would amount to about €10 per user for obliged entities (the cost of compliance, including day-to-day compliance activities). Our estimation of 500,000 users in the EU would lead to a €5 000 000 cost for the EU industry if all EU users transact with EU platforms which, given the global scale of VCs, is probably not the case. This figure would not take into account the IT development costs that would be needed in order to proceed with CDD, archiving, checking lists of terrorists etc.
It should be noted that major exchange platforms / custodians (e.g. Coinbase, Bitstamp, Circle) already have these types of solution in place, also based on "blockchain forensic tools" that help them with CDD and transaction monitoring requirements.

ATM providers would also be impacted as, to our knowledge, ATMs are not all equipped today for performing CDD. ATMs in Europe may have to be changed for CDD-compliant ones that already exist. Since the population is currently limited to about 100 in the EU, swift action would allow for lower costs to the industry (as opposed to delaying legislation in this area, by which time the number of ATMs could be much higher).

Other stakeholders would be less impacted. Software wallet providers and miners would suffer very little impact as the obligation would be placed on exchange platforms. Users would face "administrative" tasks such as providing an ID card or other documents used for verifying their identity with obliged entities but this would mainly be a one-time only identification process.

More generally, the VC industry will undoubtedly suffer from the reduced anonymity that such an initiative would bring as anonymity has been a key component of their success. Platforms and custodians that are not able to comply would have to disappear (at least from the EU market and other regulated markets such as the US) and a consolidation phase could take place, leaving a few major exchange platforms and custodians on the market, where the transactions would be concentrated, thus making their business more profitable.

On the other hand, society would be much better protected. Police forces would be able to lift anonymity in a much higher number of cases when pursuing investigations relating to suspicious transactions. Exchange platforms and custodians would participate in the control of any illicit use of VCs by reporting suspicious transactions to national authorities (one major exchange platform reported 1,000 suspicious transactions in 2015 globally for a client portfolio of 80,000). Those national authorities would be better equipped to understand and monitor the market which could, in time, lead to more confidence from all parties, rejuvenating the usage of VCs in a safer and legitimate way. Users willing to give more legitimacy to VCs would identify themselves and bring more transparency to VCs.

Member States would also be affected, as supervision and registration would have to be put in place for new obliged entities at national level. However, they already perform such tasks for a large universe of existing obliged entities; the addition of 100 additional market actors (max.) should not be particularly onerous or costly.

6.3.2.2.2 Option D - lift VCs' anonymity through the regulation of VC exchange platforms under PSD2

Effectiveness

Revising PSD2 would have the benefit of bringing exchange platforms automatically under the scope of 4AMLD and would allow broader regulatory rules, including those relating to consumer protection, to apply. However, such a move goes beyond the objectives of tackling ML/TF risks and would likely take more time to develop and agree as various provisions of PSD2 would be applied to VCs.

Costs

ML/TF related compliance would pose identical costs to option C, to which costs relating to licensing and capital requirements should also be added.

6.3.2.2.3 Comparison of options regarding exchange platforms

Objectives / impacts	Option C Exchange platforms under 4AMLD	Option D Exchange platforms under PSD2
Efficiency regarding the general and specific objectives	+++	+++
Cost	--	---
Data protection / fundamental rights	0	0
Proportionality	+	0
Conclusion	++	0

6.3.2.3 Targeting wallet providers

6.3.2.3.1 Option E - lift VCs' anonymity through the regulation of custodial wallet providers under the 4AMLD

Effectiveness

Bringing custodial wallet providers under the scope of 4AMLD would help fulfil the objective in an effective and efficient way as, similar to exchange platforms, the population of providers is limited and this option can be put in place very quickly. All exchanges through custodians would be covered (although it is hard to appreciate the percentage of total transactions that this would represent).

A major argument for this option is that it covers VC transfers that stay within the VC network and will never be converted back to FC. Given the size of the network of acceptance (110,000 merchants – 13 million wallets), this is a credible possibility.

Global-scale enforcement would have to be stimulated as this option has not yet been put forward by any international body. However, in part of the US, licensing requirements exist for these market actors (cf. New-York BitLicense).

It should be noted that major custodial wallet providers already have strong processes in place for CDD and security.

Costs

Equal to costs indicated in option C.

6.3.2.3.2 Option F - lift VCs' anonymity through the regulation of custodial wallet providers under PSD2

Effectiveness

Revising PSD2 would have the benefit of bringing custodial wallet providers automatically under the scope of 4AMLD and would allow broader regulatory rules, including those relating to consumer protection, to apply. However, such a move goes beyond the objectives of

tackling ML/TF risks and would likely take more time to develop and agree as various provisions of PSD2 would be applied to VCs.

Costs

Equal to costs indicated in option D.

6.3.2.2.3 Comparison of options regarding wallet providers

Objectives / impacts	Option E Custodial wallet providers under 4AMLD	Option F Custodial wallet providers under PSD2
Efficiency regarding the general and specific objectives	+++	+++
Cost	--	---
Data protection / fundamental rights	0	0
Proportionality	+	0
Conclusion	++	0

6.3.2.2.4 Other impacts

Considering that all of the abovementioned options limit or lift anonymity relating to VCs, this may – to a certain extent – have a dissuasive impact on the legitimate use of VCs. Also, the freedom to conduct business is a fundamental right that will in part be affected by the regulation of VC business.

Any enlargement of the scope of the 4AMLD results in increased scrutiny and thus has a bearing on the right to privacy and data protection. Any measure reducing or lifting anonymity will have a direct effect on data protection and the restriction of privacy.

However, restriction of such anonymity is considered necessary to attain the important objectives of security and ensuring a robust framework for tackling ML/TF. Moreover, obliged entities under the 4AMLD are already covered by the existing data protection framework in the 4AMLD (Chapter V).

Based on the above, from a data protection perspective, the following main elements should be taken into consideration:

- clearly justify the extension of the scope of the 4AMLD based on the demonstration of the necessity and proportionality of the new measures;
- introduce a clear definition of "VC exchange platforms" and "custodial wallet providers", and their role, so as to frame clearly which entities shall perform CDD under the 4AMLD, and consequently, will be accountable for the application of data protection safeguards;
- take into account the fact that personal data will essentially be collected digitally/on-line, and ensure that the data protection safeguards are adapted to this digital nature of the business.

6.3.2.4 Full comparison of options

Objectives / impacts	Baseline Scenario (status quo)	Non regulatory option (supra national risk assessment)	Option A Mandatory registration of users	Option B Voluntary registration of users	Option C Exchange platforms under 4AMLD	Option D Exchange platforms under PSD2	Option E Custodial wallet providers under 4AMLD	Option F Custodial wallet providers under PSD2	Comments
Effectiveness regarding the general and specific objectives **Specific objective:** Improve the detection of suspicious VC transactions and increase transparency and link them to identities	0	0	+++	++	+++	+++	+++	+++	The Baseline scenario and the non-regulatory option have been identified as ineffective or only very marginally effective to reach the general and specific objectives. All regulatory options are helping to reach the objective, with the highest efficiency for options A, C and E. Option D and F, though as effective would be less efficient as adding layers of legislation from PSD2 that are not specifically necessary to reach the objective. Option B being voluntary would probably be less effective.
Cost	0	0	-	-	--	---	--	---	All solutions imply costs. Highest cost for options D and F (licensing, capital requirements…).
Data protection / fundamental rights	0	0	-	0	0	0	0	0	Any enlargement of the scope of the 4AMLD results in in the increased amount of transition being subject to the scrutiny measures under 4AMLD and hence into interference with the right to privacy and data protection. Any measure limiting currently existing anonymity will have direct effect restricting privacy and data protection. Lifting anonymity partially (Option B) will have less effect than any option aiming at eliminating the anonymity (option A, C, D, E, F). However, restriction of the anonymity is considered necessary to attain the objectives. Furthermore, VC exchange platforms/custodial wallet providers will become obliged entities under the 4ALMD. In this respect they will be governed by the existing data protection framework in the 4AMLD (Chapter V) providing for specific data protection/retention of information safeguards when using/processing personal data for the purposes of the Directive. Also, the freedom to conduct business is a fundamental right that is impacted by the regulation of the VC business.
Proportionality	0	0	-	+	+	0	+	0	Options B, C and E are the most proportionate. All 3 would help reach the objective with the lowest costs for users and the industry. Costs for administrations would also be very limited. The self-declaration option (B) is not imposing anything on users to help fight the misuse of virtual currencies.
Conclusion	0	0	+	++	++	0	++	0	The preferred package would involve adding options B, C and E. The combined impact would be a decrease of anonymity and increase of monitoring and STRs by major gateways of the VC industry.

6.3.3 Reducing the misuse of anonymous prepaid instruments by further reducing the exemption regime for anonymous prepaid cards under the 4AMLD

The anonymous prepaid card market segment is a limited one and essentially concerns general purpose reloadable and non-reloadable prepaid cards. It represents 2% of the number of prepaid cards issued in the European Economic Area (EEA) – or about 2 million cards – and 28% of transaction values (i.e. about 5 to 6 billion euro).

Reducing anonymity for this limited segment of general purpose 'anonymous prepaid cards' will result in incremental costs for prepaid card issuers. The main costs in carrying out CDD relates to the verification of identity. The later this is carried out in the life of a prepaid card, the quicker the cost of recovery for the entity carrying out CDD.

Under the 3AMLD, a card could be reloaded up to €2 500 without having to be subject to full CDD. Under the 4AMLD, stricter rules have been imposed with a monthly threshold of €250. CDD costs are estimated by industry at 2€-3€ to 5€. Taking the upper value, this means that for a 1% beneficiary margin, up to €500 have to be spent on a reloadable card before the €5 CDD cost can be absorbed. However, this depends on the defined programmes.

The intensity of the impact on issuers will depend on the behaviour of cardholders. In the worst-case scenario, issuers (compared to today's situation), will have to support a new CDD cost. Figures would amount to less than €10.6 million[43] (for €5.4 billion transaction values or 0.2% of the yearly average nominal amount). In the best-case scenario, the recovery of the cost would in any case have been incurred under the 4AMLD but the timing of the CDD performance will now be anticipated.

The impact on the profitability of prepaid card issuers will therefore be minimal and, for the market leaders, compounded by the diversity of their prepaid card programmes. Small 'monoliners' offering general purpose reloadable prepaid cards might be more directly affected. However, the amounts at stake remain minimal.

Distributors would remain outside the scope of the 4AMLD and therefore would not be affected by the more stringent measures proposed.

Member States would not be affected in their supervisory efforts as prepaid card issuers are already 'obliged entities' under the EU AML/CFT legislation. FIUs might have to potentially address more STRs as a result of the more stringent AML/CFT requirements, but this would be in line with the objectives pursued.
As far as reloadable cards are concerned, all options with the exception of Option D are all variations on the timing of undertaking CDD (i.e. the moment in time at which CDD should be carried out). Its unitary cost will be the same if no time discounting factor is taken into account[44]. However, if carried out upfront, e.g. upon purchase of a card and the card is not used then, the issuer will have borne a cost and not necessarily recovered the full cost of CDD, depending on its pricing policies for such products.

[43] General purpose prepaid cards represent 2% of the 106 million prepaid cards issued in 2015, i.e. 2.12 million cards for a €5 CDD cost, or a €10.6 million total cost. This figure is inflated as the proportion of cards concerned encompasses both reloadable and non-reloadable cards. Under the proposed option, the AML/CFT regime for non-reloadable cards will entail no or hardly any additional CDD costs for issuers. The breakdown between both categories of cards is not available. The actual figures would be lower.

[44] Even if a time discounting factor were applied, in today's inflationary conditions, under the assumption that the CDD would have to be conducted within a few months of the purchase of the card for such a requirement to be of value, the issuer would not save much.

6.3.3.1 Option A – Suppressing all the existing exemptions of 4AMLD for prepaid instruments (i.e. suppression of Article 12 of the 4AMLD)

Effectiveness

All anonymous prepaid cards, reloadable or not, would become subject to CDD (identification and verification of the identity of the cardholder) from the first euro. This approach would eliminate anonymity – over a short period of time – and the risks related to it, addressing to a large extent the concerns expressed by law enforcement authorities. The identification of the cardholder and the registration of his/her identity would have to be carried out from the outset, either by the distributor or by the issuer upon activation of the card.

Such an approach would not necessarily need to cover all prepaid cards. Many cards/products on the market already offer degrees of identification/CDD which will allow traceability back to the user. For example, payment cards used to pay out social benefits are typically not provided to anonymous customers but, in such cases, the distributor of the card (e.g. the welfare office) will have performed customer identification already – and in such cases the card issuer is reliant on the distributor for the performance of CDD. Such cards fall outside the scope of the exemption under Article 12 of 4AMLD.

To the extent that prepaid cards, particularly reloadable prepaid cards, are seen as a substitute for a bank account, such an approach would create a level-playing field between the banking industry and the prepaid card industry with regard to the application of CDD.

The major change would concern the non-reloadable general purpose prepaid cards which today are *de facto* outside the scope of CDD. The industry believes that such a measure would negatively affect the take-up of such cards and hence could undermine more general policies on financial inclusion, notably as far as non-reloadable prepaid cards are concerned.

Costs

The cost of issuance will be seemingly higher as prepaid card issuers will have to bear CDD costs, which are estimated in some Member States at €2 to €3 per card (UK). In some Member States, where electronic verification of identity is neither widespread nor accepted, costs may reach, in some exceptional circumstances, higher amounts approaching double digit figures. According to a major card scheme and an industry association, €5 would be a reasonable assessment of today's CDD costs. The industry admits that such costs can be relatively easily absorbed when the card is used to its full effect (i.e. when a reloadable prepaid card is reloaded more than once and where non-reloadable cards are converted to reloadable ones).

Still, there may be a considerable issue of proportionality and necessity of the measure, impact on uptake (first step towards further financial inclusion) and partial substitutive effect where non-reloadable prepaid cards are concerned, when these are addressed to the general population. There is a perception that the customers of non-reloadable prepaid cards may be 'put off' by having to go through a CDD process before being even able to use the card. Issuers are of the view that they could not amortise the cost of CDD performance on low value cards. This point may be significant: in practice, non-reloadable general purpose cards bought in retail stores do not tend to carry values today in excess of €100 or £100 cards.

The risk, therefore, would be that issuers abandon either that product line or their distribution via non-banks. Today, the only interest for the major issuers is to try to get those customers to

'upgrade' their basic cards to ones with more functionalities which can be used recurrently. These are more profitable, and hence providers can better absorb the cost of a full CDD.

Negatively affecting market structure would result in lesser competition in some markets where prepaid instruments are well developed. It could also undermine efforts of financial inclusion vis-à-vis the unbanked (although this should be partially addressed in the forthcoming Directive on Payment Accounts) without necessarily addressing the AML/CTF risks, as the alternative to prepaid cards will be cash, which is nearly impossible to trace back.

Compared to the baseline scenario, costs would result from the total coverage of the whole non-reloadable prepaid card segment[45], and the anticipation of CDD costs for reloadable prepaid cards. In today's inflation conditions, the latter will have no incidence by comparison to the obligations already defined under the current 4AMLD (Article 12).

6.3.3.2 Option B - Prepaid cards when used online are subject to CDD

Such an approach would eliminate all anonymity for the online use of prepaid cards (reloadable or not).

Effectiveness

Under this option, the current €250 threshold for the use of prepaid cards in face-to-face situations would remain as it is under the 4AMLD. However, there would be no threshold anymore for the online use of prepaid cards.

This option leaves the current exemption of Article 12 of the 4AMLD unchanged for prepaid cards used in face-to-face situations. In non face-to-face environments (where cash cannot be used), prepaid cards could only be used after the cardholder had been subject to appropriate CDD measures (i.e. verified identification, through a check of phone number and address, or account number and address).

Anonymity would be lifted as is already the case for online means of payment related to a payment account (debit card, credit card or online bank transfer). This would establish a level-playing field between prepaid cards and other payment instruments.

Whilst data is not available on the respective online/offline use of prepaid cards, the assumption is that the main use of such instruments is an online one – except perhaps for security reasons (easier to conceal?) or for use by children (pocket money). Therefore, the measure proposed here would target the main uses of prepaid cards.

Furthermore, if the main use of prepaid cards is an online one, the assumption is made that the cardholder would be more willing to go through a CDD process if it is performed online, particularly if there is an incentive to buy online (lower prices, discounts e.g. on electricity bills). The chilling effect or customer inconvenience that goes with carrying out CDD at the physical point of sale would be avoided or significantly reduced – he/she identifies himself/herself online in order to conduct business online. However, such an approach has not been tested and consumer organisations have not commented on that aspect.

Leaving untouched the current situation regarding the use of prepaid cards in a face-to-face environment will not address the recurring concern of law enforcement authorities about the lesser physical detectability of plastic prepaid cards vis-à-vis cash, which when it reaches a certain bulk (banknotes) can be spotted by trained police or customs dogs.

[45] Considering the impact of legislation on the definition of that market segment, such an approach could have for effect to drastically shrink the dimension of that market and/or increase the cost of acquisition of such cards. The very existence of that market segment might be put into question.

Costs

From an economic viewpoint, prepaid card issuers are likely to consider such an approach as too costly if they have to perform CDD upon activation of the cards from the first euro or equivalent, as potentially the whole segment of anonymous general prepaid cards would be captured. CDD costs could 'eat' a significant part of the issuer's margins as far as low value prepaid cards are concerned, which will be the case for non-reloadable prepaid cards. This might therefore have a negative effect on the offer of such products on the market.

Furthermore, today, not all issuers are in a position to verify the identity of a customer at a distance as e-CDD can either not be conducted or is not accepted in all jurisdictions for the time being.

Compared to the baseline scenario, costs would result from a large coverage of the whole non-reloadable prepaid card segment[46], and the anticipation of CDD costs for reloadable prepaid cards. In today's inflation conditions, the latter will have no incidence by comparison to the obligations already defined under the current 4AMLD (Article 12).

6.3.3.3 Option C - Minimising anonymity by lowering the €250 thresholds for all prepaid cards (reloadable or not).

Effectiveness

This option consists of reducing the current thresholds of 4AMLD both for reloadable and non-reloadable cards. This would reach a balance in lowering the space for anonymity while accepting some anonymity to allow for more competition in the payment services market and to address specific needs not necessarily catered for today by most banks.

The lower the threshold, the lesser the degree of anonymity attached to a given prepaid instrument. Contrary to Option A, a lowering of the threshold with respect to non-reloadable general purpose cards might constitute a more proportionate mitigating factor.

Markets have not made full use of the €250 threshold for non-reloadable prepaid cards, as most cards sold in retail stores carry values ranging from 10, 20, 50 to 100/150 euros (or £100). A halving of the current threshold in the 4AMLD (to €125) or a return to the initial threshold of the 3AMLD (€150) would be without significant economic consequences considering today's market structure and would preserve financial inclusion by not interfering with the initial take-up phase of such products. It would avoid an' eviction effect' in favour of cash. Still, it could address the risk linked to anonymity for those cards with nominal values ranging from €125/150 to €250.

By reducing the nominal value of anonymous prepaid cards, more cards would need to be used to finance a given action, and this would therefore increase their physical detectability.

However, this approach would not allow the EU to attain a level-playing field among payment service providers (banks and non-banks) where the prepaid instrument/card is a reloadable general purpose card, as a debit card or a credit card would not benefit from an exemption if used for small monthly payments (below €250). In particular, it would also maintain a sizeable degree of anonymity in the market for those products.

[46] Considering the impact of legislation on the definition of that market segment, such an approach could have for effect to drastically shrink the dimension of that market and/or increase the cost of acquisition of such cards. The very existence of that market segment might be put into question.

Costs

Unitary costs would be the same as under Option A. However, the volume of cards captured would be lower than under Option A, and the upholding of a threshold shielding low nominal value prepaid cards (where issuers struggle to recover CDD costs) means that the impact to industry would be lower too. The cost would be less than under Option A and B.

Compared to the baseline scenario, additional costs could result from the anticipation of CDD for reloadable prepaid cards. In today's inflation conditions, this will have no incidence by comparison to the obligations already defined under the current 4AMLD (Article 12).

6.3.3.4 Option D - Minimising anonymity by applying simplified customer due diligence from the first euro and verifying identity at a later stage, e.g. upon the crossing of a threshold, e.g. €250

Effectiveness

The timing of the CDD and the intensity of the CDD procedure also has an impact on the mitigation of AML/CFT risks as well as the use of prepaid cards and related costs for the prepaid industry.

Under this Option, simplified CDD would be applied at the time of the purchase of the prepaid card. The buyer would be required to show an ID document, as is the case for the purchase of tobacco or alcohol to avoid that minors have access to such products. The actual identification and verification of identity would take place at a later stage, e.g. after some usage of the card, or upon the crossing of a threshold. (The latter aspect would have a particular impact on reloadable cards.)

The request of an ID document, an ID card, passport or else, at the point of sale could have a deterrent effect on ill-intentioned buyers without putting an undue burden on distributors that would not be required to store that information. As a consequence, such a request would not be too onerous vis-à-vis those customers who genuinely need a prepaid card.

Anonymity can only and truly be lifted after verification of identity which - under this option - in practice would only occur for reloadable cards. The identity of holders of non-reloadable prepaid cards would not be verified or even recorded at the point of sale.

Option D is a rather weak variant of Option B and Option C as a means of lifting anonymity. It is not effective, for the very fact that the identity of cardholders would be neither recorded nor verified at the point of sale and therefore a later verification of the identity would not be possible, except for repeated use of reloadable cards where such an approach would actually mean that both identification and verification of the identity would take place at a later stage.

Costs

In terms of costs, this Option is one of the cheapest. If the verification of ID is mandated after the current threshold is crossed, then the only additional operation compared to today under the 4AMLD is the obligation for the cardholder to show an ID document or equivalent at the time of purchase or of online activation of the card. This will require the maintenance of a database by the issuer to match at a later stage of the verification process, the card number, the ID of the cardholder and other information collected for the verification of ID. Option D would be more palatable than Options B and C both for industry and customers, but would not fulfil the objectives of meaningfully lifting anonymity.

Compared to the baseline scenario, this option would entail no additional costs.

6.3.3.5 Option E – All reloadable cards subject to CDD from the first euro, non-reloadable cards from a lower threshold than today

Effectiveness

This option amounts to a combination of Option B for reloadable cards and Option C for non-reloadable cards:

(i) by lowering the thresholds under the 4AMLD, by possibly reducing them from €250 to €125 or €150, as this would ensure that the EU legislation reflects current market practice for non-reloadable cards. Neither identification nor verification of identity would be requested below the threshold, thereby avoiding any chilling effect on the part of the population that buys those products essentially for shopping online. In a face-to-face situation, people will in any case continue to favour cash for their purchases. Any non-reloadable general purpose card with a value in excess of €150 or equivalent would have to be subject to CDD upon activation of the card, online or at the retail shop distributing it; and

(ii) by requesting the application of CDD (simultaneous identification and verification of identity) for reloadable cards from the first euro.

Distributors would remain outside the scope of the 4AMLD where they do not act as agents of the prepaid card issuers, which is the case for the vast majority of distributors in today's market conditions.

This approach presents the merit of preserving current market functioning, including from a financial inclusion perspective as far as non-reloadable cards are concerned, whilst imposing similar AML/CFT requirements for reloadable general purpose prepaid cards as to bank accounts which are subject to full CDD at the time of their opening.

At the same time, the lower threshold imposed on non-reloadable cards has for effect that in inflationary times in future, the growth of that market segment will be constrained, thereby naturally reducing a segment qualified by the anonymity of its products.

Costs

The lowering of the current AML/CTF threshold, for instance from €250 to €125 or €150, would leave prepaid card issuers unaffected for the time being, as market needs for non-reloadable cards would still be served without having to perform CDD and having to support related costs.

The main impact concerns reloadable general purpose prepaid cards, which are the closest means of payment to a debit card linked to a payment account, which under today's AML/CFT requirements is subject to a full CDD.

Compared to the baseline scenario, additional costs could result from the anticipation of CDD for reloadable prepaid cards. In today's inflation conditions, this will have no incidence by comparison to the obligations already defined under the current 4AMLD (Article 12).

6.3.3.6 Comparison of options

Objectives / impacts	Baseline Scenario (status quo)	Non-regulatory options	Option A All prepaid cards subject to CDD from 1st euro	Option B Prepaid cards (reloadable or not) when used online subject to CDD from 1st euro	Option C Reducing the €250 threshold (both for physical and online uses) to €150 for all cards	Option D Requiring SDD from 1st euro and verification of ID beyond a threshold (e.g. €250)	Option E All reloadable cards subject to CDD from 1st euro, all non-reloadable cards above €150	Comments
Effectiveness regarding the general and specific objectives **Specific objective:** to reduce the misuse of anonymous prepaid instruments	0	0	++++	++++	++	+	+++	The Baseline scenario and the non-regulatory option have been identified as ineffective or only very marginally effective to reach the general and specific objectives. All regulatory options are helping to reach the objective except for the baseline scenario, with the highest effectiveness for options A, B, C and E. Option D is not sufficiently efficient.
Cost	0	0	---	--	-	0	--	All options imply additional costs. However, most prepaid card issuers have in place the necessary staff and IT systems to conduct customer due diligence. Option A in covering the whole universe of anonymous general purpose and would therefore be a costly one. An important dimension in this respect is the capacity of the issuer to absorb those costs, and this for a large extent will depend on the chosen business model (payment of an upfront fee or not) and the use (renewed or not) made by the cardholder of the payment instrument. Concretely, the earlier the performance of CDD in the life of the card, the higher the risk of non-cost recovery if the card is little used afterwards.
Data protection / fundamental rights	0	0	-	0	0	0	0	Any enlargement of the scope of the 4AMLD results in in the increased amount of transition being subject to the scrutiny measures under 4AMLD and hence into interference with the right to privacy and data protection. Any measure limiting currently existing anonymity will have direct effect restricting privacy and data protection. The more effective the measure is with respect to lifting anonymity, the greater the impact on privacy and data protection rights of users of the cards. The options with least negative impact on data protection are the least effective to attain the objectives pursued. . In this context it should however be flagged that all options build upon already existing exemptions with regard to prepaid instruments

								laid down in article 12 of the 4AMLD. In this respect they will be governed by the existing data protection framework in the 4AMLD (Chapter V) providing for specific data protection/retention of information safeguards when using/processing personal data for the purposes of the Directive. Also the fundamental right to conduct business will be impacted, given the cost and resource impact on obliged entities. This right will be less impacted by options C and E (mainly focussing on further lowering the existing threshold) then by the other options.
Market effect	0	0	----	---	-	-	--	The market effect is systematically negative except for the baseline scenario which would satisfy the industry. It includes two components: the effect for the industry and the effect for the customers.
Financial inclusion	0	0	----	-	-	0	-	All solutions imply a negative effect for financial inclusion. Option A is likely to have a large detrimental effect on the market in terms of financial inclusion, as it could lead to the termination of the issuance/distribution of low value prepaid cards. Options B, C, and E create small inconvenience for the poorest users.
Conclusion	0	0	0	++	+	0	++	The three negative effects of the options are weighted in order to be comparable to the positive effect. The most efficient option regarding this cost/benefit analysis would be option B combined with Option C. Option E is a variant of the combined Options B and C. It is however less effective with regard to the objective of lifting anonymity regarding the online use of non-reloadable prepaid cards.

NB: The assessment of cost, market, data protection and financial inclusion impacts are summed up, then divided by 4, rounded up and then compared to the assessment of the effectiveness of the options.

How to limit risks of circumvention related to the use of foreign prepaid cards?

Whatever the option retained, there is a risk of circumvention that needs to be addressed, for the new EU rules to be efficient.

The AML/CFT rules are territorial by nature and the 4AMLD only applies to the territory of the EEA. Global card schemes have the ability to impose geographical – as well as sectoral - restrictions on the use of prepaid cards. Such restrictions could be imposed by Member States for cards issued in the EEA47. However, cards issued by foreign issuers would remain out of the reach of the Member States AML/CFT authorities. It should be noted that the US require that prepaid cards that can be used outside their territory are fully subject to CDD from the first dollar.

The only European point of attachment in the present case would be the merchants to whom the 'foreign' cardholder would buy goods and services and the banks of the merchants that would treat the card payments (the 'acquirers'). Neither the merchants nor their banks are obliged to accept foreign cards. In practice, cards issued by the global card schemes (AMEX, Diners, MasterCard, Visa) will usually be accepted, likewise in major cities for national cards such as e.g. JCB for Japan or China Union Pay held by their citizens holidaying in Europe. The global cards schemes already have robust AML/CFT rules as they are also keen to preserve their major asset, namely their brand. Besides those major players, there are a series of domestic card schemes throughout the world. However, their global acceptance by merchants or the banks of those merchants is likely to be very limited. It suffices to have a look at the European market where domestic cards absolutely need to be co-branded with a global scheme to be accepted abroad, including in the Union. De facto, the likelihood that a merchant accepts a card issued in an exotic jurisdiction48 by an unknown prepaid card issuer is very low, if not minute.

The question may nevertheless be asked whether prepaid cards should not be refused when issued in jurisdictions with low AML/CFT standards in this respect. Clearly, merchants have the ability to discriminate among would-be consumers depending on the country of issuance of the card and a number of them do so in the e-commerce context. This is an issue that the Union is currently addressing for intra-EU trade in goods and services. However, could merchants do so from an AML/CFT perspective, when they are not in the scope of the EU AML/CFT legislation? Probably not, but their banks could as they already are in the scope of that legislation and have as 'acquirers' to accept and treat those payments made with prepaid cards. Banks could therefore refuse to accept payments made with prepaid cards issued in jurisdictions that would not have equivalent AML/CTF requirements vis-à-vis prepaid cards. This would simply require upgrading the software of card terminals at the merchants' points of sale.

A global approach would consist in convincing the FATF of the need to issue stricter AML/CFT standards to minimize the anonymity risks related to some prepaid cards for global spread in future. A more immediate action could be to define at EU level equivalence conditions to determine which foreign jurisdictions have equivalent requirements to those of the EU regarding prepaid instruments.

6.3.4 Improving FIUs' access to - and exchange of - information held by obliged entities

6.3.4.1 Option A – Aligning EU law with the latest international standards in the field and clarifying FIU powers in the 4AMLD

Effectiveness

This option (resulting in a direct access of FIUs to information held by obliged entities, and this independent of any prior STR) has the merit of adjusting at the margin the current regulatory framework (very limited changes to the existing text are required), but in a way that is meaningful, as the proposed legal modifications will effectively enhance the powers of the FIUs concerned. By clarifying FIUs legal obligations, it ensures that the provisions are

[47] For reference, the Belgian banking industry 3 or 4 years ago took the decision to block –unless otherwise requested by the cardholder- the use in some foreign jurisdictions of debit and credit cards issued in Belgium due to increase card fraud risks in those territories that do not apply the 'chip & pin' security technology.

[48] There is a tenacious story among law enforcement authorities, a 'legend' according to the prepaid card industry about a card issued in a Central American country known for its offshore banking activities that would have reached the shores of Europe with $250.000 on it. However, this, to our knowledge, has not been corroborated by public evidence.

effectively applied by all Member States, thus harmonizing their powers to obtain relevant information, which will also facilitate the exchange of such information within the EU. It does not create a fundamental overhaul of the system and provides more clarity for FIUs when implementing the provisions of the 4AMLD. Furthermore, it ensures alignment with international standards in this field and reinforces a global approach.

Since this option is relatively consensual (based on our consultation), it could be rapidly adopted and implemented by Member States and thereby would support a swift adoption process of the planned amendment of the 4AMLD without delaying its adoption. It would not entail any significant change to data protection rules nor the protection of fundamental rights, especially the right to security. In this respect, the following safeguards already expressed in the previous Opinion of the EDPS of 2013 shall apply: (i) in case of data exchange between FIUs, the retention period of the data exchanged should be limited to what is strictly necessary in relation to the purpose of the processing, (ii) the update of data needs to be ensured by designated responsible agents within the FIUs, and (iii) the way to ensure security of data processed should be specified. Moreover, the investigative powers and the data access prerogatives of the FIUs should be clearly defined by law (accountability), data subjects should be informed that their data in possession of obliged entities may be transferred to an FIU, and the public policy purpose of the processing should be stated.

Effective implementation still relies on Member States following a transposition process which entails a risk of late or incorrect transposition.

Costs

This option does not entail any major costs. It simply clarifies the scope of information from obliged entities that is accessible to FIUs – which is cost neutral. The direct access to information held by obliged entities would bring some marginal savings by removing in certain Member States the role of a third party in requesting the information.

6.3.4.2 Option B - Establish a single European FIU to receive, analyse and disseminate results to national competent authority

Effectiveness

Under this option, a single European FIU would be competent for obtaining, directly at its request, any information held by obliged entities in the event of a suspicion of ML/TF. As analysed in the Impact assessment of the 4AMLD, this option would be more suited to an integrated EU financial market, and would also be arguably the most efficient and effective way to combat ML and TF across the EU, by allowing a more holistic overview across the Internal Market. As such, it would contribute in protecting the public policy objective of security. It would also overcome the current cooperation difficulties which exist between national FIUs. Finally, it would rely on an instrument that is directly applicable (Regulation) which would increase its effectiveness.

However, this approach may raise concerns among Member States about sovereignty and would require fairly far-reaching changes to Member States' rules and existing arrangements. It would be likely to delay a rapid adoption of the amended 4AMLD and negatively affect the possibility of rapidly fixing the regulatory framework to address other risks.

It would also lead to a central storage of data relating to STRs in a comprehensive way. Even though it may increase accountability and data control, it may impact more profoundly data protection of customers being subject to STR reporting. Therefore, access to such a database should be adequately framed, which would at least include applying all the data protection safeguards that are currently applicable at national level (cf. Option A) at the level of the European FIU.

Costs

As addressed in the Impact assessment of the 4AMLD, this option would require additional funds to be made available at EU level for setting up such an agency. However, these costs would be offset by savings made at national level following the transfer of the tasks carried out by Member State FIUs. The pooling of resources could also represent some long-term savings for the global AML/CFT system.

As currently there is no EU body that has completely replaced (and removed) all national authorities, there exists no benchmark/comparable scenario for a cost estimate. Therefore, it is not possible to estimate the overall cost for this option (e.g. expected gains at national level).

6.3.4.3 Comparison of options

Objectives / impacts	Baseline scenario (status quo)	Non-regulatory options	Option A Aligning with international standards and clarifications in 4AMLD	Option B creating a single EU FIU to obtain information	Comments
Effectiveness regarding the general and specific objectives **Specific objective:** Improve FIUs' access to – and exchange of – information held by obliged entities	0	0	+	++++	The baseline scenario has been identified as not effective, and the non-regulatory options will not allow for a swift improvement of the AML/CFT framework. In any case, as they are non-regulatory, they cannot provide the concerned legal clarifications. The two regulatory options are helping to reach the objective of improving access to - and exchange of - information by FIUs. The highest effectiveness is reached by option B. Option B would be more suited to an integrated EU financial market, and would also be arguably the most efficient and effective way to combat ML and TF across the EU, by allowing a more complete overview of the situation across the Internal Market. It would also overcome the current cooperation difficulties which exist between national FIUs.
Cost	0	0	0	+	The baseline scenario and non-regulatory options: no costs. Option A entails no additional cost since it only clarifies the authority and competences of FIUs. Option B requires some costs for setting up a single EU FIU and adapting national systems to the new process. Those short-term costs would be offset by the savings made at national level in removing Member States FIUs. In the long term, the AML/CFT system would benefit from economies of scales.
Data protection / fundamental rights	0	0	0	-	The baseline scenario and non-regulatory options: no effect. As option A merely aims at clarifying an already existing obligation, it entails no change from a data protection/fundamental right point of view. In this respect the existing data protection framework in the 4AMLD (Chapter V) providing for specific data protection safeguards/retention of information provisions, when using/processing personal data for the purposes of the Directive fully applies. Option B requires giving the authority to a single EU FIU to access, receive and process data held by obliged entities regarding their customers. It would lead to a central storage of data relating to STRs in a comprehensive way. As such it raises the issue of necessity and proportionality of such measure. On the other hand, it ensures a better accountability and control by having a single regime for data protection.
Proportionality	0	0	++	- -	The baseline scenario and non-regulatory options: no noticeable effect. Option A only represents a marginal adjustment of the legal framework. Hence it would allow to rapidly fixing known issues at short term. The solution should be rather consensual between Member States and easy to implement. This approach would therefore facilitate a rapid adoption of the amendment of the 4AMLD. Option B represents a radical change which would be more effective, but at the same time more complex for adapting systems. It may raise concerns among Member States about sovereignty and require quite far-reaching changes to Member States' rules and existing arrangements. Hence it would probably delay a rapid adoption of the amendment of the 4AMLD. It would also negatively affect the possibility of rapidly fixing the regulatory framework to address the other risks.
Conclusion	0	0	+++	+	Option A offers the best approach to reach the objective at the lowest possible cost. It represents only a marginal change to the current system and should be consensual since it aims at further aligning EU law with international standards. Hence it is easy to implement and would contribute to a swift adoption of the proposed legislation.

6.3.5 Providing FIUs (and potentially other AML/CFT competent authorities) with an efficient mechanism to ensure timely access to information on the identity of holders of bank and payment accounts

6.3.5.1 Option A – an automated central registry at Member State level, directly accessible to national FIUs (and other national AML/CFT competent authorities) for AML/CFT purposes

Effectiveness

This option would offer an efficient mechanism for national FIUs to have a timely access to information on the identity of holders of bank and payment accounts, thus enabling them to build at national level a full picture of all financial transactions conducted by persons involved in suspicious transactions. Such nationally available information can also be exchanged cross-border – spontaneously or upon request – with other EU or non-EU FIUs, using the existing cooperation mechanisms.

The effectiveness of such registries was also confirmed by the stakeholder consultation. All Member States where FIUs had access to such registries, indicated that these were an extremely valuable tool in the fight against ML and TF, as it allows for the swift identification of financial assets, the tracing back of funds to their owners, the freezing or monitoring of accounts and transactions, and the enforcement of financial sanctions.

Through the centralised approach, this solution also tackles both the problem of fragmentation of information, and the problem of swift access to information by FIUs. FIUs will be able to directly enter their query into the registry and instantly obtain the results, thus avoiding costly and time-consuming blanket requests or non-action.

As this single registry can be directly fed by credit and financial institutions that are already legally obliged to identify their customers on the basis of documents or information obtained from a reliable and independent source (article 13 of the 4AMLD), the risks of material/identification errors should be very limited.

Finally this targeted approach by FIUs - only requesting further information from the relevant credit and financial institutions when needed - will also focus attention to customers/financial transactions that may potentially be linked to ML and TF activities. This will help them to more easily identify higher risk situations, and further monitor such high risk clients or transactions in a closer and more targeted way. More generally, this will enable them to better mitigate their reputational risks (linked to unknowingly performing banking services to criminals or terrorists), which will have a positive effect on the cost/benefit of their risk monitoring processes.

Costs

The creation of a central registry generates two types of costs for Member States: one-off costs to set up the registry, and recurring costs for the use of the tool.

The one-off costs mainly consist of acquisition costs for hardware, software and labour linked to the:

- initial development of the IT tool
- first alimentation and implementation of the IT tool

The recurring costs mainly consist of the costs for software, hardware and labour costs linked to the:

– maintenance, updating, functioning of the IT tool

– access/consultation of the IT tool

On the costs involved, reference is made to Annex 7 for more details. We received information from 5 Member States that have put in place a registry allowing them to identify holders of bank and payment accounts, or that are in the process of putting one in place. Although this data does not allow us to draw reliable statistical conclusions on this issue[49], it does give a rough estimate/indication of the range of such costs. On the basis of the information received, one-off costs range from €170 000 to €1 000 000, and yearly recurring costs range from €3 000 to € 600 000.

These costs should be compared with the higher total annual costs linked to blanket requests for FIUs and the financial sector (cf. Annex 7 for more details), ranging from appr. €94 000 to appr. €245 000 000[50].

Other impacts

Taking into account the fact that such registries would centralise personal data relating to natural persons, the need to flank such measures with necessary safeguards from a data protection/fundamental rights perspective would have to be considered.

From this perspective, it is also worth highlighting that this option also allows FIUs to focus only on the relevant credit and financial institutions when examining and analysing suspicious transactions, thus avoiding the untargeted dissemination of personal data to the financial sector.

In line with the Digital Rights Ireland judgement (C-239/12), EU directives setting up automated central registries at national level processing personal data should also impose minimum safeguards for protecting data subjects' rights, in particular relating to the purpose, data retention, time and access. In this respect it should be recalled that the 4AMLD already establishes an obligation upon Member States to set up central registries processing personal data relating to natural persons (cf. articles 30 and 31), and contains a chapter on data protection (Chapter V). Furthermore, the storage of data into these registers should be limited to the minimum data necessary to the purpose (see also Annex 7 in this respect), the concerned data subjects should be informed that their data are recorded and accessible by FIUs (or other AML/CFT competent authorities), and be given a contact point for exercising their rights of access and rectification. It is also indicated to provide for a maximum retention period for the personal data in these registries (see also Annex 7 in this respect). Moreover, access to such registries should be limited as much as possible on a "need to know" basis.

6.3.5.2 Option B – an automated central mechanism at Member State level, directly accessible to national FIUs (and, as the case may be, other AML/CFT competent authorities) for AML/CFT purposes

This option encompasses Option A, but is wider and more flexible allowing choice as to the IT architecture (which could take various forms, ranging from a central registry (option A) to

[49] The Member States that were able to provide us with information on the costs is only a small group. Some of them were not able to provide a detailed cost figure on their registry, and only gave a rough estimate or prospective figures. Member States also pointed out other elements which can influence the comparability of both the one-off costs as the recurring costs, such as the scope of the registry not being identical to that of option A, labour cost calculated in a different way (ranging from internal labour cost to invoice cost for delivered services), etc..

[50] Hypothetical lowest cost according to Annex 7: Cyprus = hypothesis batched request + costs financial sector. Hypothetical highest cost according to Annex 7:The Netherlands = hypothesis separate requests + costs financial sector.

a central automated data retrieval system), which is left to the discretion of Member States to determine. This means that Member States that already have such mechanisms in place (or are in the process of setting them up) can simply continue to use these IT tools, while those who will have to set them up in the future will be able to opt for the IT solution of their choice. Therefore, globally, Option B has a positive impact on the cost aspect and the policy choices for Member States.

As the impacts of the central registry were already discussed above, the assessment of the impacts below will solely focus on the automated central data retrieval system.

Effectiveness

A central data retrieval system would offer the same advantages as a central registry as far as the timely access to information on the identity of holders of bank and payment accounts by FIUs and the issue of fragmentation of the information are concerned. As mentioned under option A, it will also allow FIUs to focus on relevant credit and payment institutions, thus avoiding costly blanket requests, and help the institutions concerned to manage their risks more effectively.

A central data retrieval system is not directly fed by the primary source (credit and financial institutions), but will allow FIUs to consult/retrieve - through a centralised portal – existing information in other databases or IT tools. The information contained in the underlying databases/IT tools can be supplied by different private or public actors (credit and financial institutions, national authorities (e.g. tax authorities), …), thus offering a certain degree of flexibility regarding the source of information.

As data retrieval systems are based upon other underlying IT-tools (e.g. existing databases, registries, etc…), Member States will have to ensure that all these components are kept up to date and are in compliance with relevant legislation (amongst which data protection legislation). This could generate some indirect costs.

Costs

The creation of a central retrieval system generates two types of costs: one-off costs to set up the system (setting up of an IT-portal), and recurring costs for the use of the system.

The one-off costs mainly comprise the acquisition costs for hardware, software and labour linked to the:

- initial development of the IT-portal
- interconnection with underlying databases or IT tools and implementation of the IT-portal

The recurring costs mainly comprise the costs for software, hardware and labour costs linked to the:

- maintenance and functioning of the IT-portal
- access/consultation of the IT-portal

Currently, only one Member State has a retrieval system in place allowing the identification of bank and payment accounts holders[51]. The one-off costs of this system amounted to appr.

[51] Another Member State is in the process of building such a system.

€1 200 000, while the recurring costs amount to appr. €480 000 per year. This information is too limited and depends upon a too wide variety of parameters to draw hypothetical conclusions on the costs such a tool could generate for other Member States.

Other Impacts

Same as Option A.

6.3.5.3 Option C – an automated central registry or mechanism at Member State level, directly accessible to a broader range of national authorities and for a broader purpose

Effectiveness, costs and other impacts

This option would offer the same advantages as options A and B, topped by the fact that the registry would also be available to a broader range of national authorities for a broader purpose. Although the one-off costs and recurring costs are the same as under option A and B, the cost/benefit ratio would improve, as the registry/automated mechanism would serve a wider purpose.

As this option allows to meet the general and specific objectives, it is assessed under the current impact assessment. However, notwithstanding the above, this option also goes beyond the objective of this proposal, which is limited to the use of such tools for AML/CFT purposes, by providing FIUs (and as the case may be, other AML/CFT competent authorities) with a swift access to relevant information on the identity of holders of bank and payment accounts. Moreover, providing access to such automated mechanism for purposes other than AML/CFT should be further examined from a data protection and proportionality perspective, especially taking into account the "purpose specification principle" (avoidance of the use of the information for secondary, incompatible purposes and avoidance of use by third parties with unrelated competences). In addition, security measures should be enacted, in order to avoid unauthorised access and data theft or leakage.

Option C is a policy option that deserves further reflection and analysis, but one which cannot be implemented through the amendments to the 4AMLD because the latter is based on article 114 of the TFEU and its scope is limited to the prevention of the use of the financial system for the purposes of ML and TF. In order to implement option C, which is a wider option including judicial law enforcement, a self-standing Directive would be needed, which goes beyond the scope of this impact assessment examining proposals to modify the 4AMLD. In this respect, reference can be made to the Commission's Action Plan for strengthening the fight against terrorist financing, where the possibility of a self-standing legislative instrument to allow for a broader consultation of bank and payment account registers for other than AML/CFT investigations and by other authorities is one of the policy solutions which is currently under exploration.

Finally, it would be remiss not to point out recent events[52] which underline the importance for the EU to have effective instruments to combat opacity facilitating ML and tax evasion. Council Directive 2014/107/EU[53] and the wider international framework on automatic exchange of financial account information between tax authorities aims at ensuring that as of next year national tax authorities obtain comprehensive information related to income and assets held abroad by their residents. This Directive and related instruments are based on the

[52] https://panamapapers.icij.org/

[53] http://ec.europa.eu/taxation_customs/taxation/tax_cooperation/mutual_assistance/direct_tax_directive/index_en.htm

provisions in the 4AMLD[54]. In order to verify whether CDD provisions are correctly applied by financial institutions, in particular the identification of beneficial owners of entities and arrangements, and to be able to ensure that the information being reported to the Member State of residence is accurate and complete, tax authorities would need access to the above mentioned central registries or central automated mechanisms for the identification of holders of bank and payment accounts.

[54] https://www.oecd.org/tax/automatic-exchange/

6.3.5.4 Comparison of options

Objectives / impacts	Baseline Scenario	Non-Regulatory measures	Option A central registry	Option B central mechanism	Option C central registry or mechanism for broader access/ purpose	Comments and analysis
Effectiveness regarding the general and specific objectives **<u>Specific objective:</u>** to improve swift access by FIUs to relevant information on the identity of holders of bank and payment accounts to avoid (i) the use of blanket requests that are costly and delay the collection of such information, or (ii) the non-action linked to lack of efficient mechanisms to collect the information	0	0	++++	++++	+++	Baseline scenario: the baseline scenario has been identified as not effective with regard to the specific and general objectives. Non-regulatory option: this might only very marginally improve the situation with regard to the baseline scenario, but will not address the specific and general objectives either. Options A and B are both equally effective to address the general and specific objectives: they will be implemented through the modification of the 4AMLD, and (i) improve swift access by FIUs to relevant information on the identity of holders of bank and payment accounts, (ii) avoid costly and time consuming blanket requests or non-action by FIUs. Option C will also allow to reach the general and specific objectives, but will have to be put in place through a self-standing Directive. Therefore, using this option will take more time to reach the objectives, making it less effective than Options A and B.
Cost-efficiency **<u>Reduction of costs:</u>** o costs for the FIUs, linked to the collection of the information (sending out blanket requests to all the banks and payment institutions) o costs for the financial sector, linked to analysing and answering to unnecessary requests d the financial sector **<u>Investment costs:</u>**	0	0	++	++	+++	Baseline and non-regulatory option: these options would not entail any set-up-costs, as the status quo would remain entirely/almost entirely unchanged. However, Member States that currently do not have any central registry/mechanism will have to continue sending costly blanket requests. Options A and B generate set-up (one-off) costs ranging from €170 000 to €1 200 000, while yearly recurring costs range from €3 000 to €600 000. These costs are to be compared to the higher total hypothetical annual costs linked to blanket requests for the FIU + the financial sector, ranging from appr. €94 000 to appr. €245 000 000. Option C will have a better cost/benefit ratio, as the infrastructure put in place can be used by more authorities for a wider purpose.

One-off costs and recurring costs for setting up an automated registry or mechanism. **Benefits:** Prevention of ML and TF, and recovery of assets.						
Data protection/fundamental rights: **Registries/mechanisms:** For holders of bank and payment accounts that are natural persons, the registries/mechanisms will contain personal data, which will be made accessible to FIUs and, as the case may be, other AML/CFT competent authorities. **Blanket requests:** If no registries/mechanisms are available, blanket requests can be sent, disseminating in an untargeted way personal data to the financial sector.	0	0	0	0	-	For Member States that currently do not have registries/mechanisms in place the baseline and non-regulatory option will result in the dissemination of personal data in a non-targeted way to credit and payment institutions, which may create problems from a data protection perspective. Options A and B allow for a targeted approach as far as the consultation of personal data is concerned. However, the central access by FIUs and other AML/CFT competent authorities to personal data of holders of bank and payment accounts needs to be adequately framed, and other safeguards for fundamental rights and data protection would have to be considered. In this respect, the 4AMLD (Chapter V) already provides for certain data protection/retention of information safeguards for the use of personal data for the purposes of the Directive. Option C also allows for a targeted approach as far as the consultation of personal data is concerned. But this option also allows a broader range of authorities to consult the personal data, for a wider purpose, than options A and B. Option C cannot be implemented under the 4AMLD, and needs to be established through a self-standing Directive. Providing access to such registry/mechanism for purposes other than AML/CFT triggers issues with respect to the "purpose specification principle", data protection and proportionality. An adequate data protection framework covering a broader access to the registry/mechanism would be needed.
Proportionality	0	0	++	++	-	The baseline and non-regulatory option: sending out blanket requests to all concerned credit and payment institutions to trace the holders of bank and payment accounts raises proportionality issues form the angle of time, cost and data protection. Options A and B both offer a targeted approach, which allows for proportionate action regarding time, cost and data protection perspective. Option C would go beyond the specific objective.
Conclusion	0	0	+++	+++	++	Options A and B are both easier to put in place and more proportionate than option C and, after insertion in the 4AMLD, they are already covered by the data protection chapter in this Directive.

7. DISCARDED OPTIONS

On the **improvement of the effectiveness of the EU policy towards high-risk third countries**, three discarded options were examined of which one was based on the listing of examples of enhanced CDD measures (discarded for its little added value), and another on harmonizing the countermeasures at EU level (discarded on the basis of proportionality).

On the issue of **lifting/reducing anonymity regarding VCs**, two additional options were discarded, consisting in (i) a full prohibition of the use of VCs in the EU (considered detrimental for digital innovation and progress), and (ii) the regulation of miners (which would generate enforcement problems and stifle innovation).

Regarding **prepaid cards**, three further options have been examined and discarded, the first two because they represented a level of detail not suitable for EU law and the third one because it is considered lacking both effectiveness and efficiency. The application of an absolute limit on the value that can be uploaded on a prepaid card has not been retained, as prepaid cards whose nominal values or reloadable capacity exceed the CDD thresholds defined today by the 3AMLD and tomorrow by the 4AMLD are subject to CDD. The risk of anonymity is lifted in those circumstances. Furthermore, the global card schemes apply commercial caps on those cards (varying between 10€ and 20.000€). In the same way, the possibility to request by law that a new card, embossed with the name of the cardholder, is issued at the time of conversion of a non-reloadable card into a reloadable card (the closest proxy to a debit card) has not been retained. This measure is considered best left to the national level or to the card schemes themselves. The possibility of bringing retail distributors of prepaid instruments in the scope of the relevant EU legislation has not been retained either, on grounds of both proportionality and effectiveness.

On **FIUs access to – and exchange of – information held by obliged entities**, only one discarded option - the establishment of a European FIU - was examined and discarded pending the result of the FIU mapping exercise.
Finally, on **FIUs access to information on the identity of accountholders,** four discarded options were examined, of which the main options consisted in putting in place a decentralised mechanism at Member State level (discarded for being not effective enough) or an EU registry/mechanism (discarded for being too complex and time consuming).More information on the discarded options is provided in Annex 8.

8. PREFERRED OPTION

8.1 Improving the effectiveness of EU policy for high-risk third countries via a harmonised EU approach for enhanced due diligence measures to be applied by Member States and obliged entities

Operational objective	The preferred option
To improve the effectiveness of the list of high-risk third countries by providing for a harmonised approach at EU level with respect to enhanced due diligence measures to be applied by Member States	Option B – to include, in the EU framework, a prescriptive list of enhanced customer due diligence measures and an illustrative list of countermeasures, and require from Member States and obliged entities to apply at least all the ECDD measures and/or, where appropriate, one of the countermeasures when dealing with high-risk third countries designated by the Commission. This option reaches the objective of enhanced monitoring of the financial transactions involving listed countries as it will impose to obliged entities the obligation to apply the same level of ECDD measures to a specific list of high-risk third countries.

8.2 Improving the detection of suspicious virtual currency transactions and increasing their transparency by linking them to identities

Operational objective	The preferred option
Increasing the transparency of virtual currency transactions / linking transactions to an identity	Option B, C and E are the preferred options and should be combined to maximise their effects. All 3 are needed in order to achieve the objective as they address 3 major components of the VC market: users, exchanges and wallets. Leaving any of these players out would drastically reduce the efficiency of any action.

8.3 Reducing the misuse of anonymous prepaid instruments by further reducing the exemption regime for anonymous prepaid cards under the 4AMLD

Operational objective	The preferred option
Reducing the misuse of anonymous prepaid instruments by further reducing the exemption regime for anonymous prepaid cards under the 4AMLD	The preferred option is a combination of Option B 'suppressing thresholds upon online use of prepaid cards' and Option C 'lowering the current threshold'. This combination presents the merit of treating like with like. By suppressing the threshold for the online use of prepaid cards, a level playing field is established vis-à-vis debit cards and credit cards which are already subject to CDD. Anonymity is lifted with no risk of flight to cash, as the latter can seldom be used online (except in a few Member States where cash payment on delivery is still a common practice). As CDD will be conducted online in most jurisdictions, there will be no 'chilling' effect vis-à-vis consumers. This combination also addresses the face-to-face use of prepaid cards. In reducing the current threshold (Option C), the space for anonymity in face-to-face uses of prepaid cards is theoretically reduced in a proportionate way. Option C avoids a flight from prepaid cards to cash for face-to-face uses as it aligns the current legislative threshold of €250 with the actual market practice where non-reloadable cards rarely exceed €150. The combination of Options B and C is more effective than Option E as it covers a greater population of prepaid cards, by suppressing the CDD exemption for non-reloadable prepaid cards, which is preserved under Option E.

8.4 Improving FIUs' access – and exchange of – information held by obliged entities

Operational objective	The preferred option
To improve FIUs' access to – and exchange of – information held by obliged entities by clarifying FIUs powers to obtain this information.	Option A is the preferred option, by aligning the current provisions of the 4AMLD with the latest international standards on obtaining additional information from obliged entities. The provisions would also be clarified to request direct access by FIUs to information held by obliged entities as part of the core task of a FIU and facilitate information exchange. This approach presents the merit of changing only marginally the regulatory framework, while increasing the effectiveness of access and exchange of information. The solution is rather simple to implement and would bring some marginal savings in certain Member States by simplifying the procedures. This solution is also based on an international consensus widely shared among stakeholders. Hence this approach would facilitate a rapid adoption of the amending of the 4AMLD on this point.

8.5 Providing FIUs (and potentially other AML/CFT competent authorities) with an efficient mechanism to ensure timely access to information on the identity of holders of bank and payment accounts

Operational objective	The preferred option
To provide FIUs with an efficient mechanism to get timely access to information on the identity of holders of bank and payment accounts	Based on the analysis of the impacts of the different options, option B should be preferred. This option would require Member States to put in place at national level an automated centralised mechanism, such as central registries or central data retrieval systems, to which national FIUs (and, as the case may be, other national competent authorities) can have direct access to obtain the necessary information to swiftly identify the holders of bank and payment accounts. Option B is efficient with regard to the general and specific objectives as it would: – improve swift access by FIUs to the information required, thus avoiding the use of costly and time consuming blanket requests or non-action by FIUs due to lack of efficient mechanisms; – allow for a targeted approach – including from a data protection perspective – with respect to initial and additional information requests towards credit and financial institutions; – enable FIUs to swiftly trace criminal and terrorist financing flows – both nationally as cross-border through the existing EU FIU-collaboration – thus enhancing the transparency of these flows, which contributes to the prevention of ML and TF. Option B offers more flexibility to Member States than option A as regards the choice of the IT tool to reach the objective. Under option B, tools can range from a central national registry to a central national data retrieval system, or even include other automated centralised mechanisms that meet the objective. This will also enable Member States that already have such centralised mechanisms in place to maintain their existing tools. Option C is a policy option that deserves further reflection and analysis, but goes beyond what is targeted by the objectives and cannot be implemented through the amendments to the 4AMLD, as the scope of the latter is limited to the prevention of ML and TF. In order to implement option C, a self-standing Directive would be needed.

On the basis of the tables and explanations outlined in chapters 6 and 8, the combined assessment of the preferred options can be summarized as follows:

	Lifting or reducing anonymity/enhancing transparency of criminal or terrorist financing flows at EU level	**Improving detection of suspicious transactions by obliged entities at EU level**	**Directly[55] improve financial intelligence (including exchange of information) at EU level**	**Directly[56] protect the EU internal market from AML/CFT threats posed by high-risk third countries**	**Cost/Benefit[57]**	**Data Protection and fundamental rights**	**Prevent ML/TF by more effective detection of such financing flows**
Enhanced CDD towards high-risk third countries (option B)	+++	+++	N/A	+++	-/+++	0	+++
Virtual Currencies – transparency (combined options B, C and E)	+++	+++	N/A	N/A	--/+++	0	+++
Prepaid instruments – transparency (combined options B and C)	+++	++	N/A	N/A	--/+++	0	++
FIUs – align to FATF standards: improve access to and exchange of info (option A)	+	0	+++	N/A	0/++	0	+++

[55] Only direct effects are taken into account. However, all of the initiatives can/will have an indirect positive effect on this.

[56] Only direct effects are taken into account. However, all of the initiatives can/will have an indirect positive effect on this.

[57] i.e. costs versus the quantitative and qualitative benefits that will be generated by reaching the specific objective.

Access of FIUs to identity accountholders (option B)	++++	+	++++	N/A	--/++++	0	++++
COMBINED IMPACT	+++	++	+++	++	--/+++	0	+++
COMMENTS	All five preferred options will have a relatively high impact on this criterion, which will further reinforce the global transparency of ML/TF financial flows. The transparency of financial flows constitutes the first step of the preventative system, allowing – in a second step – obliged entities to monitor these financial flows more efficiently.	The detection of suspicious transactions by obliged entities constitutes the second step in the ML/TF preventative system. The chief objective to improve financial intelligence (which is the third step in the chain) is positively impacted by those preferred options that directly involve "obliged entities", as they are the "feeders" of the preventative ML/TF system and the key to helping strengthen the fight against ML/FT. By transmitting more information and qualitatively better STRs to the FIUs, they will enhance financial intelligence.	The third step in the preventative chain is Financial Intelligence. Financial intelligence is indirectly improved by the two previous steps (transparency of financial flows and detection of suspicious transactions by obliged entities). Moreover, it is also directly improved through the two preferred options reinforcing the powers of FIUs. These two improvements – especially when combined – will give FIUs a fuller picture on the criminal and terrorist financing financial flows.	This objective is only directly improved by the first preferred option. However, the primary aim of this option is to further harmonize EU legislation in order to avoid loopholes/weak spots at EU level that can be exploited by terrorists and criminals. Therefore this option has a clear focus on the protection of the EU internal market.	The main costs are related to access of FIUs to information on account holders (setting up of IT tools), and the compliance of the VC sector with the 4AMLD. However, both options are also considered to be very effective as regards the general and specific objectives. Therefore, globally, the benefits outweigh the costs. Moreover, the IT tool relating to information on accountholders will have a positive effect on the access and exchange of information by FIUs within the EU.	The 4AMLD (Chapter V) already has specific data protection/retention of information safeguards in place regarding the use of personal data for the purposes of the Directive. These provisions will automatically apply to all of the five preferred options. Also, the automated mechanisms for access to information on the identity of accountholders will allow for a more targeted approach in this field as compared to the baseline scenario (mainly blanket requests to the financial sector).	The combination of enhanced powers of FIUs on the one hand (preferred options 4 and 5), and the limitation or reduction of anonymity/enhanced transparency regarding VCs, prepaid instruments and high-risk third countries on the other (preferred options 1, 2 and 3) will lead to a more effective detection of illicit flows while improving preventative action in this area.

9. MONITORING, TRANSPOSITION AND EVALUATION

According to article 67 of the 4AMLD, Member States shall bring into force law, regulations and the administrative provisions necessary to comply with the 4AMLD and immediately communicate these texts to the Commission.

Considering the fact that the transposition period of the 4AMLD is still ongoing, due care should be given to take into account as much as possible work already undertaken by the Member States when implementing and transposing obligations that are closely linked to the issues set forth in Part 1 of this impact assessment, such as for example the exemption regime for pre-paid cards.

Where appropriate and on request, the Commission services will offer assistance to Member States, throughout the implementation period of the 4AMLD, for the implementation of the legislative changes in the form of transposition workshops with all the Member States or through bilateral meetings.

According to article 65 of the 4AMLD, the Commission will conduct an evaluation of the extent to which this directive has been implemented in the Member States. By modifying the 4AMLD, this evaluation will also include the implementation of the measures that Member States have taken to achieve the general and specific objectives set out in Section 4 (see table).

The targeted modifications to the 4AMLD relating to Part 1 of this impact assessment can be monitored according to the following specific indicators:

Objectives	**Indicator**	**Source of info**
Improve the detection of suspicious transactions relating to high-risk third countries	- Number of STRs filed with regard to suspicious transactions - Estimates of increased filings compared to the baseline scenario - Number of ML/TF files transmitted by FIUs to enforcement authorities, involving such transactions	- National FIUs
Improve FIUs access to – and exchange of – information held by obliged entities. Improve FIUs access to relevant information on the identity of holders of bank and payment accounts. Avoid (i) the use of blanket requests, or (ii) non-action by FIUs.	- Number of direct requests for additional information from FIUs towards obliged entities - Estimates of increased filings compared to the baseline scenario - Timeliness of access by FIUs to information on the identity of holders of bank and payment accounts - Number of consultations of the automated mechanism by FIUs - Number and typology of ML/TF files transmitted by FIUs to enforcement authorities, where automated mechanisms to verify the identity of holders of bank and payment accounts have been consulted	- National FIUs and authorities responsible for the registers or retrieval systems
Improve the detection of suspicious	- Number of STRs filed by VC exchange	- National FIUs and

VC transactions	platforms and custodial wallet providers - Number of ML/TF files transmitted by FIUs to enforcement authorities, where VCs were involved - Number of self-declared users.	European Banking Authority
Reduce the misuse of anonymous prepaid instruments for the purpose of ML/TF	- Number of STRs filed relating to such products - Number of ML/TF files transmitted by FIUs to enforcement authorities, where prepaid instruments are involved - Estimates of the decrease of such files - The development of the market segment relating to the prepaid instruments covered by the amendments - including consumer behaviour and the effect on financial inclusion	- National FIUs - Consultations and data collection of market actors and consumers relating to market developments and consumer behaviour

Furthermore, the Commission will also work with the joint Committee of the European Supervisory Authorities on AML (AMLC) - which, amongst others, produced reports on the implementation of the 3AMLD in some specific areas – in order to monitor the application of the new legislative framework. The Expert Group on the Prevention of Money Laundering and Terrorist Financing (EGMLTF), could also serve as a forum for sharing information on application issues.

There is no target date or time frame for when these objectives will be reached. The objectives are to improve the prevention and detection of ML and TF and to ensure that the EU framework is effective. As a consequence there will be an on-going monitoring of these results that may feed into the Article 65-report on the implementation, but more likely it will help the Commission to assess the efficiency overtime and help prepare future revisions of the EU framework. The collection of this information (indicators) is largely required to review the effectiveness of the Members States' AML/CFT systems (Article 44 4AMLD). It will therefore not result in an extra administrative burden for Member States.

The 4AMLD allows Member States to adopt or retain in force stricter rules in the field covered by the directive (within the limits of EU law) and the Commission will pay particular attention to measures that are stricter that those presented in this Impact assessment.

Monitoring of the application of the 4AMLD will also take place indirectly through the mutual evaluation processes of the FATF (15 EU Member States are members of this body) as well as Moneyval (the other 13 Member States are members of this body). This peer review process is an essential and rigorous process to ensure that Member States comply, both in law and in practice, with FATF international standards. The 4 AMLD has been aligned, where appropriate, with these International standards and evaluations take place approximately every 5-7 years for each country and can be complemented by follow-up reports, usually every 2 years. The FATF is placing increased emphasis on the assessment of effectiveness of measures, as opposed to compliant legal frameworks. The mutual evaluations concerning individual EU Member States will represent an important element for the Commission's own evaluation of the effectiveness of the legal framework.

As these monitoring options would make use of the existing European or International structures and would not require the setting up of a new instrument, they would entail limited cost at EU level.

As regards progress indicators for the key objectives, good ratings in FATF or Moneyval reports on EU Member States would be useful indicators of the consistency of the EU approach with international standards and of the preservation of the EU financial system's reputation.

A transposition plan relating to the 4AMLD was agreed with Member States at the first transposition workshop on 27 September 2015. In the meantime, all 5 planned workshops have taken place according to scheme, and the need for any additional bilateral assistance is being examined.

Taking into account the issues raised during the transposition workshops, it is plausible to assume that transposition challenges may occur in relation to (a) mechanisms that will ensure that FIUs have access to the identity of holders of bank accounts and (b) Beneficial Ownership registers (in view of the amendments/options outlined in part 2 of this impact assessment). The Commission may consider organising additional workshops that will focus on these issues.

The fact that the 4AMLD is not yet transposed makes it difficult to analyse transposition and compliance issues with regards to the current initiative.

Moreover, the acceleration of the transposition of the 4AMLD (by the end of 2016 instead of mid 2017) may be a challenge when the amending directive may have a later deadline.

The Inception Impact Assessment indicates that no new implementation plan will be established as this initiative will extend or build upon the already existing implementation plan. An amended transposition plan will follow the proposed legal text on inter-service consultation.

Part II

1. BACKGROUND AND POLITICAL CONTEXT

The proposals set forth in this section of the document go beyond the Action Plan. They are a direct consequence of the recent financial scandal denominated Panama papers and of the political momentum created by it.

The reviews of the Savings Directive[58] (2008 and 2012) previously identified the use of legal entities and arrangements and the setting-up of such structures in places like Panama and the BVI, reaching conclusions similar to those brought to light by the Panama papers. In 2009 the Commission proposed an amendment to the Savings Directive[59] to address use of intermediary structures, albeit with a limited scope. However, such proposal did not have political support. The Directive on Administrative Cooperation[60], as revised by Directive 2014/107/EU, replaced the Savings Directive as of January 2016, and implemented at EU level the new international standard on automatic exchange of information for tax purposes.

Recent disclosures by international media (the so-called "Panama Papers" and previous similar investigations) confirmed the conclusions of the Savings reviews and highlighted significant deficiencies in the worldwide financial system and the potential need for further improvements to the anti-money laundering framework of the EU. Careful consideration needs to be given to issues mainly related to gaps in the standards of keeping records of beneficial ownership[61] information of intermediary entities to identify potential deficiencies in the effectiveness of the customer due diligence (CDD) obligations of financial institutions. The transparency of beneficial ownership information is one of the key topics which will be addressed in the Anti-Corruption Summit on 12 May 2016 in London.

On 14 April, the EU G5 countries (DE, ES, FR, IT and UK) issued a statement on the need for action as regards beneficial ownership information. It calls for the application of enhanced standards of transparency, committing to establish beneficial ownership registries requiring that such information is made available to tax administrations. As a first step, a pilot initiative for automatic exchange of such information is launched. The statement also called on the OECD, in cooperation with the Financial Action Task Force (FATF), to set up a new single global standard for such exchanges. As a next step, a system of interlinked registries on beneficial ownership information should be set up, mandating those organisations to develop common international standards in the field.

In addition, the G20 statement of 18 April calls on "the FATF and the Global Forum on Transparency and Exchange of Information for Tax Purposes to make initial proposals by our October meeting on ways to improve the implementation of the international standards on transparency, including on the availability of beneficial ownership information, and its international exchange".

[58] Council Directive 2003/48/EC of 3 June 2003 on taxation of savings income in the form of interest payments.
[59] Council Directive 2014/48/EU of 24 March 2014 amending Directive 2003/48/EC on taxation of savings income in the form of interest payments
[60] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation
[61] Beneficial ownership is the term used for the ultimate natural persons who own/control an entity or legal arrangement, as opposed to an intermediary entity or a nominee.

The European Commission also submitted an information note to the 22/23 April informal ECOFIN Meeting asking for Member States views on measures to strengthen the framework on anti-money laundering in order to further increase transparency, focussing on the link between tax evasion, aggressive tax planning and money laundering. In response, Finance ministers were of the opinion that the revision of the 4AMLD should go beyond the amendments announced in the Action Plan, calling for action in particular to enhance the accessibility of beneficial ownership registers, to clarify the registration requirements for trusts, to speed up the interconnection of national beneficial ownership registers, promote automatic exchange of information on beneficial ownership, and strengthen customer due diligence rules[62].

In order to implement these measures, Directive (EU) 2015/849[63] (4AMLD) could be the appropriate legal instrument.. The customer due diligence on financial accounts, which will enable the automatic exchange of financial account information, is carried out since 1 January 2016 under Directive2011/16/EU[64] (the Directive on Administrative Cooperation). That Directive implements the Global Standard on automatic exchange of financial account information in tax matters which relies extensively on information collected for anti-money laundering purposes under the 4AMLD. Consequently, any enhancement of the rules and requirements relating to the access to, and accuracy of, beneficial ownership information directly benefits and strengthens the operation of the existing automatic exchange of financial account information. The proposals brought forward to amend the 4AMLD we designed to make the most of the synergies obtained from the operation of the two Directives.

2. OVERALL SITUATION AND OBJECTIVES

The Panama Papers and earlier findings in the Offshore Leaks in 2013[65] have revealed that offshore jurisdictions are often used as locations of intermediary entities that distance the beneficial owner from the assets for various reasons and often for tax evasion. One leaked memorandum from a partner of Mossack Fonseca said: "Ninety-five per cent of our work coincidentally consists in selling vehicles to avoid taxes."[66] The information made public suggests that intermediary entities were used to obscure and dilute the AML obligations between the financial institutions and the trust and company service providers, often with the purpose of tax evasion[67].

The leaks mention that for the 40-year history Mossack Fonseca had around 14.000 clients and assisted in establishing 214.000 offshore trust and companies. It also emerged that European banks are among the top ten institutions that used the services of the Panama trust and company service provider.

---

62 http://english.eu2016.nl/documents/publications/2016/04/22/informal-ecofin---line-to-take-nl-presidency

63 Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing , OJ L 141, 05.05.2015, p. 73.

64 As modified by Council Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation, OJ L 359, 16.12.2014, p. 1.

65 Offshore leaks is a similar journalist investigation by the ICIJ disclosing details of 130,000 offshore accounts in April 2013, for more information, visit https://offshoreleaks.icij.org/

66 http://www.theguardian.com/news/2016/apr/03/the-panama-papers-how-the-worlds-rich-and-famous-hide-their-money-offshore

67 See for example https://assets.documentcloud.org/documents/2783029/20160404-banks-03.pdf

The relationship between EU banks and the use of offshore intermediary entities while obscuring information on the actual owner of the account can be addressed at EU level, because the customer due diligence measures in the 4AMLD and the Directive on Administrative Cooperation apply to all customers of EU obliged entities and financial institutions, irrespective of the customer's place of establishment, thereby raising no issue of extraterritorial effect.

Tax evasion and aggressive tax planning are global problems, as is money laundering. These European banks used the services of the Panamanian trust and company service provider, to set up intermediary entities in places such as the BVI or inconspicuous New Zealand, with a view to obscure and dilute AML obligations, so as to hide the beneficial owners behind such entities and often evade taxation.

Global Standard on Automatic Exchange of Information

The newly adopted Global Standard on Automatic Exchange of Information (AEOI) developed by the OECD and to be monitored by the Global Forum on Tax Administration is meant to reduce such possibilities for tax evasion by revealing formerly undetected cases. It is based on the exchange of financial account information with tax authorities in the account holders' (and sometimes their beneficial owners') country of residence. Under the Standard, financial institutions are obliged to collect and report information to their jurisdiction on accounts held by non-resident individuals and entities and, when those entities are Passive Non-Financial Entities, their beneficial owners, collectively referred to as Reportable Persons. That information is then transmitted to the jurisdiction where the Reportable Persons are resident. The Standard prescribes the customer due diligence procedure to be followed by financial institutions for the identification and determination of the tax residence of the Reportable Persons, and was built upon the AML/CDD procedures, which determine the standard of knowledge as regards the beneficial ownership of the financial accounts.

The Global Standard is implemented in the EU by way of a substantial extension of the Directive on Administrative Cooperation and is applied as of 1 January 2016 by 27 Member States (Austria has a 1-year derogation). As foreseen in the Global Standard, the customer due

diligence procedure in Annex I to the Directive relies extensively on information collected for AML purposes, which is governed by the 4AMLD). Therefore, any enhancement of beneficial ownership information directly benefits the operation of the Automatic Exchange of Information.

The 4AMLD brings upgraded standards of customer due diligence and an expanded scope of beneficial ownership information. However, there are areas where there is clear scope for further improvements in order to better tackle offshore tax evasion in view of the evidence of the Panama papers and related cases.

3. EU RIGHT TO ACT AND SUBSIDIARITY

The legal basis of the initiative will be article 114 TFEU – see in detail section 3 of the Impact Assessment.

Further to the international dimension of tax evasion, tax planning and money laundering, EU action is important to put pressure on third countries, leading by example. The G5 initiatives on the tax area (first on the implementation of the global standard and now on exchange of beneficial ownership information) are good examples of how an initiative led by EU Member States secures global impact.

The standard of knowledge on beneficial ownership needs to be consistent throughout the EU so as to keep a level playing field between Member States and ensure the cohesion of the internal market. If left to national legislation, distortions would undoubtedly follow, since these measures target specific market operators with crucial economic relevance which no MS would want to encumber or in any way put in a less favourable position. Additionally, since the reporting under the Directive on Administrative Cooperation relies on the information collected pursuant to the AMLD, any bias in the implementation of the rules would also lead to additional distortions within the EU.

Despite the setting up of complex structures, frequently the money and assets never left the European financial institutions holding the accounts, but only changed account holders, therefore being subject to the EU legal framework.

4. POLICY OBJECTIVES

General Objective	– To prevent Money laundering and terrorist financing by greater transparency on capital flows
Specific objectives	– To enhance transparency and improve public access to the beneficial ownership registers for legal entities and legal arrangements
	– To build on the improvements on access to beneficial ownership information in the 4AMLD that apply to all new customer relations and improve the monitoring of existing beneficial owners of existing customers like trusts, other legal arrangements and legal entities such as foundations to prevent circumvention of existing EU transparency standards.
	– To reduce the possibility for entities with no active business to circumvent the existing 25% threshold and hide their beneficial ownership
	– To align the understanding and application of how trusts should be registered and monitored in the EU

5. POLICY OPTIONS AND ANALYSIS

5. 1. **Certain** intermediary entities are particularly susceptible to hide illicit money

5.1.1. Need to update the beneficial ownership information for certain trusts, other legal arrangements and legal entities such as foundations (systematic review and monitoring of certain existing customers)

5.1.1.1 Problem Definition

Offshore intermediary entities, like trusts, other legal arrangements and legal entities such as foundations are often used to distance the beneficial owner from the assets for various reasons and often for tax evasion and other illicit purposes. The EU and global instruments to tackle that issue are respectively the Directive on Administrative Cooperation and the Global Standard on Automatic Exchange of Financial Account Information. Those instruments rely extensively on information collected for AML purposes.

The 4AMLD contains important improvements to the beneficial ownership information on trusts, other legal arrangements and legal entities such as foundations. Those improvements apply to all new customer relations, but not systematically to all existing customer relations. The non-systematic monitoring of the existing beneficial owners of existing customers like trusts, other legal arrangements and legal entities such as foundations would allow circumvention of existing EU transparency standards found in the Directive on Administrative Cooperation and an opportunity to hide illicit money.

Figures on dimension - prevalence of offshore intermediary entities

The involvement of offshore centres both at the level of provision of financial services directly to clients and at the level of providing suitable locations for setting up intermediary entities that then use the services of the onshore financial sector have been extensively documented in the Second review of the Savings Directive[68]. The analysis relies, amongst others, on publicly available statistics from the Swiss National Bank[69] and aggregate statistics of the Bank of International Settlements (BIS)[70], supplemented at the time with bilateral statistics from the BIS, obtained on a non-disclosure basis. While there is no proof in the statistical data that those intermediary structures always facilitate tax evasion, the problem definition outlined above and the evidence leaked in the Panama papers show that such intermediary structures are often used for tax evasion[71].

Findings from the Swiss national bank

The publication "Banks in Switzerland" encompasses some very detailed geographical and/or client breakdowns in Table 38 "Fiduciary business, by country". The definition of fiduciary business for the purposes of the "Banks in Switzerland" report can only be found in the 1997

[68] http://ec.europa.eu/taxation_customs/resources/documents/taxation/personal_tax/savings_tax/savings_directive_review/swd_2012_16_en.pdf

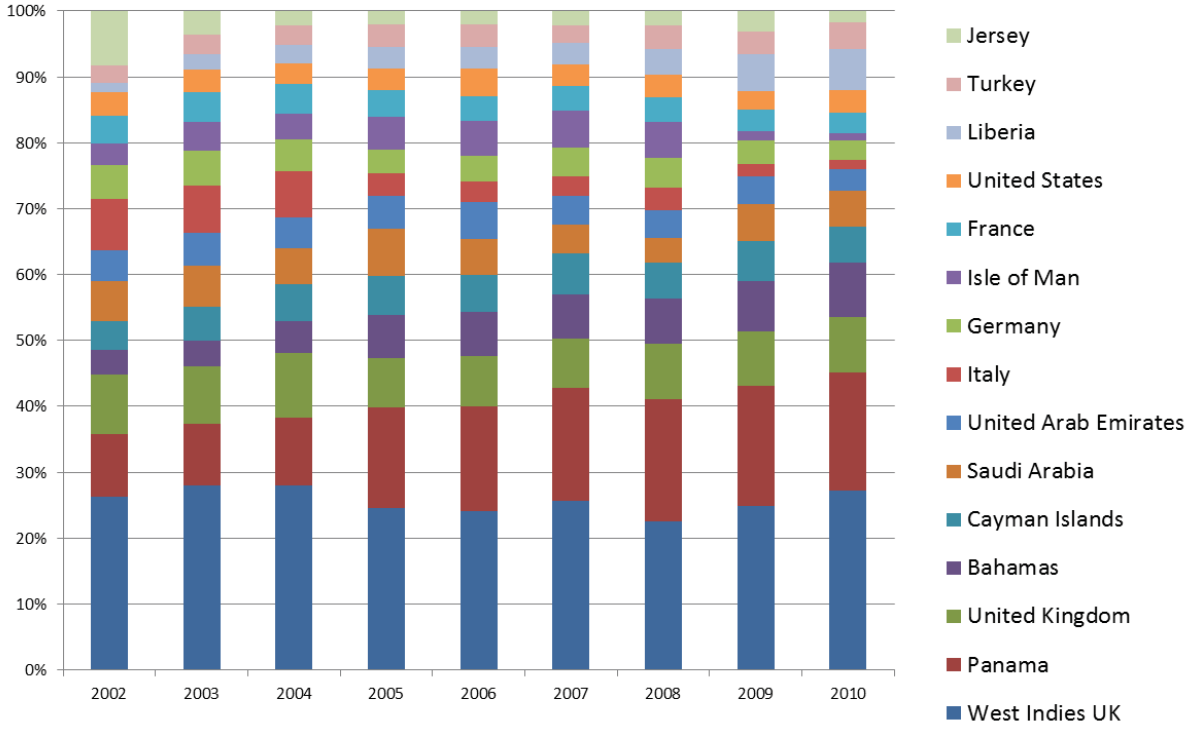
[69] General link to the publication http://www.snb.ch/en/iabout/stat/statpub/bchpub/stats/bankench
The important data sources are as follows (links the PDF versions, which are less detailed, but provide a better quick overview on the scope)
http://www.snb.ch/ext/stats/bankench/pdf/deen/Stat32.pdf
http://www.snb.ch/ext/stats/bankench/pdf/deen/Stat38.pdf
http://www.snb.ch/ext/stats/bankench/pdf/deen/Stat38c.pdf

[70] http://stats.bis.org/statx/toc/LBS.html

[71] https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf

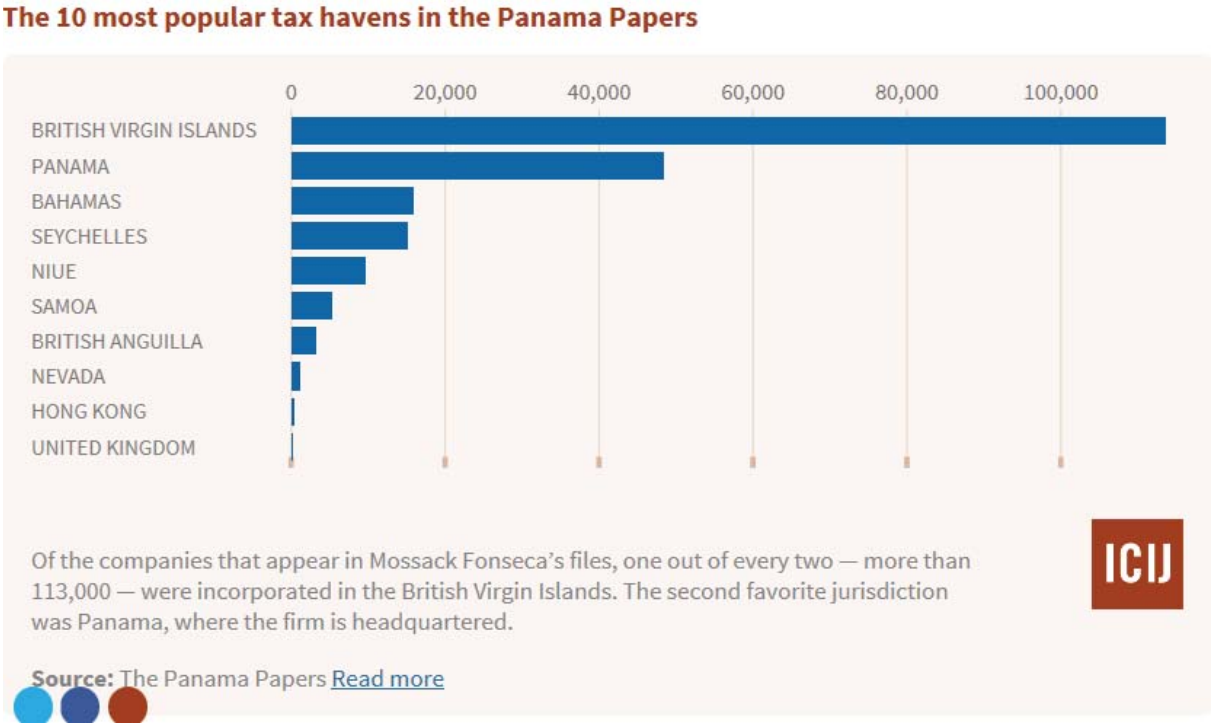
edition of the publication, which is not available in English, so the definition is an unofficial translation.[72] From the definition it is clear that fiduciary business consists primarily of **deposits from non-residents (fiduciary liabilities)** that are afterwards re-deposited abroad in the name of the bank, but for the account of the depositor.

The geographical breakdown and ranking for fiduciary liabilities is very important. There are 8 countries that may be considered as offshore centres among the first 15 countries and they represent an average of **67% of the fiduciary liabilities peaking to CHF 163 billion in 2007** attributable to that group (the share of West Indies UK, i.e. **British Virgin Islands alone is almost 26%** on average, with **Panama being second with around 20%** and **Bahamas around 10%**).



That exact same pattern, involving the **BVI, Panama and Bahamas** is present in **exactly the same order and almost exactly the same shares**, in the **Panama Papers** leak which shows more than 113.000 offshore trusts and companies having been created in the BVI, almost 50.000 in Panama and around 17.000 in Bahamas.

[72] Fiduciary transactions include investments, loans and equity interests which the bank holds or grants in its own name, but for the account and at the risk of the customer, on the basis of a written agreement. The instructing customer bears the full currency, transfer, price and collection risks and is the exclusive beneficiary of all accruals from such transactions; the bank only charges a commission. Fiduciary funds received by the banks mainly come from abroad and are almost exclusively invested abroad. They essentially consist of short term foreign investments in third banks or in branches legally dependent on Swiss banks. In the latter case, these transactions must appear in the balance-sheet, since they involve a commitment from the branch towards the head office in Switzerland.



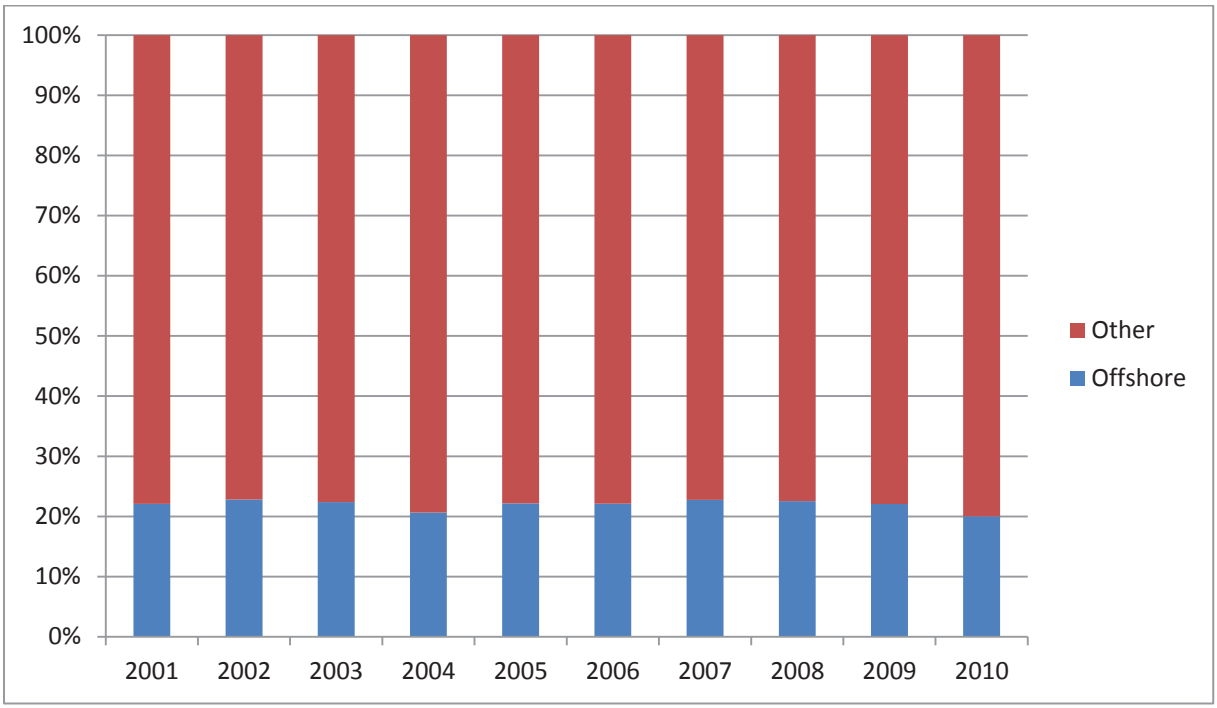
The information from the Swiss National Bank is the most detailed public source that is available. We do not have that level of detail in publicly available statistics in the EU and can only show the aggregate data for the whole EU in the information from the Bank of International Settlements (see below). Nevertheless, it can be reasonably concluded that some Member States would have similar patterns to the Swiss statistics, because the locations of intermediary entities for Swiss banks follow very closely the findings of the Panama Papers.

Findings from the Bank of International Settlements

The International Locational Banking Statistics of the Bank for International Settlements (BIS) includes quarterly data on assets and liabilities of domestic banks and branches of foreign banks situated in the 43 reporting countries broken down on a bilateral basis according to the counterparty country of their foreign counterparts. A breakdown of the data by sector and country of residence of counterparty, and country of the reporting banks is available. The sectorial breakdown includes liabilities to non-banks. Nevertheless, it is not possible to differentiate between deposits from individuals, non-bank financial entities and commercial entities or other structures within the total amount of the non-bank balances[73].

The analysis in the Second Review of the Savings Directive, based on a breakdown per counterparty jurisdiction, showed that the **share of accounts of offshore non-banks in EU banks is around 20%,** peaking to **around USD 1 trillion for 2007**.

[73] The latest BIS data have some non-country-specific aggregates for a breakdown of the non-banks share into other financial corporations and non-financial corporations, but no country-specific data.



Some of those accounts would be attributable also to non-bank financial entities. The latest BIS statistics[74] show that, based on aggregate data for all jurisdictions, around **50% of the liabilities are towards non-bank non-financial entities**.

Prevalence of discretionary trusts among offshore intermediary entities

Whether the intermediary entity would take the form of a trust, another legal arrangement, a foundation or a corporate has historically been tied to the type of legal system in place. In particular, in the UK Crown Dependencies and the UK Overseas Territories, trusts have been one of the most common ways of distancing the originator from the assets and both the beneficiaries of those assets and the proceeds.

The definitions of various types of trust vary depending on the type of trust jurisdiction. Generally, a trust is considered "irrevocable" when the settlor (if formally giving away control over the trust and the trusts' assets) cannot revert back to him. It is considered "discretionary" when the trustee has varying powers of discretion to either identify a specific beneficiary out of a class of beneficiaries, or "smaller" discretion as to when, how much and in what proportions a beneficiary would become entitled to a discretionary distribution from the trust. While in theory they could be used for legitimate purposes too, discretionary trusts are particularly "useful" for hiding illicit money, because the settlor, after contributing the assets to the trust, may claim that he has no control over the trust. In addition, until the discretion is exercised, individual beneficiaries may also not be identifiable.

There are no official statistics on the share of discretionary trusts in all types of trusts, but public statements of industry representatives can be used as an indication:

- A Guide to British Virgin Islands Trusts by Palladium Trust Services[75]

  "Most British Virgin Islands trusts tend to be discretionary trusts."

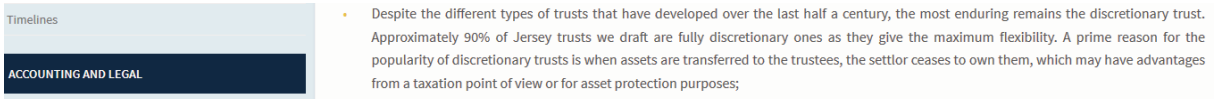
[74] http://stats.bis.org/statx/srs/table/a3.1
[75] http://www.palladiumtrustservices.net/PDFs/Palladium%20Guide%20to%20BVI%20Trusts.pdf

10. Types of Trusts

10.1 Discretionary trusts

Most British Virgin Islands trusts tend to be discretionary trusts. These are trusts in which the distribution of capital and income between beneficiaries is at the discretion of the trustees, with the result that no beneficiary is entitled to call on the trustees to distribute capital and income. If the terms of the trust allow it, the trustees may not be obliged to pay out capital or income to any of the beneficiaries for the entire perpetuity period of the trust (for further information on Perpetuity Periods, see paragraph 11 below).

- Jersey Trust Formation by Healey Consultants[76]
  "Approximately 90% of Jersey trusts we draft are fully discretionary ones as they give the maximum flexibility […] the settlor ceases to own them, which may have advantages from a taxation point of view"



5.1.1.2. Problem drivers

Background - treatment of discretionary trusts under the EU AML Legislation

Under the 4AMLD, the definition of beneficial owner of trusts, other legal arrangements and legal entities such as foundations covers a broader range of information than it was the case under the repealed Third Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (3AMLD)[77]. While the definition under the repealed 3AMLD only covered settlors and beneficial owners when those had significant ownership and control (above 25%), the new definition under Fourth AMLD covers the settlor, the trustees, the protector, if any, the beneficiaries or where the individuals benefitting from the legal arrangement or entities have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates and any other natural person exercising ultimate control over the trust by means of direct or indirect ownership and by other means. The Directive imposes as part of the compulsory customer due diligence measures Art 13 (1)(d):

[…]conducting ongoing monitoring of the business relationship and […] ensuring that the documents, data or information held are kept up-to-date

It also provides in Article 14(5) that the obliged entities shall

[…]apply the customer due diligence measures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis, including at times when the relevant circumstances of a customer change

The available evidence on the size of the potential problem outlined in points 2.1.1 and 2.1.2 reveals that (irrevocable) discretionary trusts are widely used in jurisdictions like the BVI, for

[76] http://www.healyconsultants.com/jersey-company-registration/trust/
[77] Directive 2005/60/EC, OJ L 309, 25.11.2005, p. 15

example. As stated there, while in theory they could be used for legitimate purposes too, they are particularly "useful" for hiding illicit money, because the settlor, after contributing the assets to the trust, may claim that he has no control over the trust. In addition, until the discretion is exercised, individual beneficiaries may also not be identifiable.

While some settlors and individual beneficiaries of discretionary trusts were not covered under the 3AMLD. The new definition of the beneficial owner of trusts under the 4 AMLD would always allow the settlor and any beneficiaries to be considered as beneficial owners of the trust. However, while this new definition applies across the board to new customers under Article 14(1), any monitoring for existing customers is applied "at appropriate times" and "on a risk-sensitive basis" under Article 14(5). Thus, although the change of definition raises the standard of knowledge as regards the beneficial ownership of certain customers like trusts, other legal arrangements and legal entities such as foundations, the 4 AMLD requirement does not require that existing customers are systematically reviewed.

This raises the question of how those customers, which are already existing and not new customers, should be monitored under this new definition. The fact that a settlor may not be identified until the customer due diligence is undertaken under the 4AMLD means that the potential source of the funds/assets, where the risk is usually found, cannot be assessed reliably until such a systematic review is performed. In view of the wide use made of discretionary trusts in certain jurisdictions posing a challenge, the lack of systematic monitoring according to the new definition of beneficial ownership on existing customers can be problematic in certain cases as it may not allow detecting and assessing risks on time in certain cases.

It has been revealed in the Panama Papers that detecting and assessing the risk on time and reacting to it may be hindered, intentionally or unintentionally[78]. The findings reveal that offshore intermediary entities have been servicing sanctioned regimes for years until a full review was triggered:

> It was not until August 2015 — more than a year after sanctions against Pangates had been announced — that Mossack Fonseca acknowledged the blacklisting and scrambled to find ownership details, utility bills or any other identifying information from the Dubai administrators of Pangates and Maxima Middle East. Mossack Fonseca finally reported that the companies were on international sanctions lists to Seychelles regulators in August 2015.
>
> Although he had long been a customer of Mossack Fonseca, the firm's emails at the time record no mention of the sanctions. That changed in 2010, when British Virgin Island authorities demanded information on Drex Technologies S.A., a company owned by Makhlouf that Mossack Fonseca had incorporated ten years earlier. Mossack Fonseca employees looked for — and quickly found — information that had circulated widely for years, including details of Makhlouf's political ties and alleged smuggling.
>
> "It is a decision that may be 12 years too late," added another employee, Daphne Durand, "but one that must be taken in light of the circumstances."

[78] https://panamapapers.icij.org/20160404-sanctioned-blacklisted-offshore-clients.html

That partner, Chris Zollinger, wrote colleagues that "there are allegations (rumors), but not any facts or pending investigations or indictments." He noted a colleague's earlier notes from a conversation between Mossack Fonseca and HSBC, the UK-headquartered bank that served as Makhlouf's financial manager, in which the bank assured the law firm that HSBC's Geneva and London offices "know about Mr. Makhlouf and that they are comfortable with him."

If HSBC didn't have an issue with him, Zollinger said, "then I think we can also accept him."

The scope of the automatic exchange of information

As explained in "2. Problem Definition", the customer due diligence under the Directive on Administrative Cooperation (DAC2) relies extensively on identification and beneficial ownership information collected for AML purposes practically for all types of reportable accounts upon their initial review and in case of "change in circumstances". In particular, for the identification of Controlling Persons of intermediary entities (referred to as Passive Non-Financial Entities in the Directive, for short Passive NFEs) the Reporting Financial Institutions rely on information collected and maintained for AML purposes.

Based on that identification, the Directive then prescribes additional steps in order to determine whether a Controlling Person of a Passive NFE is a Reportable Person. For accounts above the equivalent of USD 1.000.000, the Financial Institution is obliged to obtain a written document, called "self-certification" from the Passive NFE that contains, *inter alia*, information on the tax residence of the Controlling Persons of that Passive NFE. **That self-certification does not contain beneficial ownership information allowing the identification of any additional beneficial owners**, because, as stated, the identification of beneficial owners relies on information collected and maintained for AML purposes.

Any reduced scope of beneficial ownership information under AML affects directly the reporting under the Directive on Administrative Cooperation. Therefore, the non-systematic monitoring of the existing beneficial owners of existing customers like trusts, other legal arrangements and legal entities such as foundations would allow circumvention of existing EU transparency standards found in the Directive on Administrative Cooperation and an opportunity to hide illicit money.

The objective is to increase the scope of application of the improved rules on beneficial ownership under the 4 AMLD.

5.1.1.3. Regulatory options

Option 1 - Baseline scenario - no action

Enhancement of the AML and transparency legislation

No action would lead to the continued potential circumvention of existing EU transparency standards found in the Directive on Administrative Cooperation and a continued opportunity to hide illicit money.

Option 2 – An obligatory systematic review of all existing customer relations by all obliged entities

Under this scenario, the customer identification-related information for all existing customer relationships would have to be reviewed across the board by all obliged entities and within a specific deadline.

Enhancement of the AML and transparency legislation

This option would bring all customer relations to the standard envisaged in the 4 AMLD in a large-scale exercise. It does not rely on a distinction between the types of entities or the balance of the accounts and to that extent would meet the objective with greater certainty.

Costs and administrative burden

The associated administrative burden of such a large-scale review across the board by all obliged entities for all their clients might be significant. That would involve setting up a separate system for reaching out to each existing customer and asking for an update of the beneficial ownership information, then monitoring the compliance of the customers with that request and taking measures where necessary.

Data protection and fundamental rights

This option would encompass a large set of personal data. The data include identification and details on all settlors and beneficiaries of all trusts that are customers of obliged entities. That information could be used to fight money laundering, but it would also be the basis for tackling the problem of tax evasion by way of automatic exchange of information.

Proportionality

While this option provides for a comprehensive screening of existing customers and thus a broader overview, its effect may not be proportionate to the overall cost of implementation and the desired objective to target specific customers.

Option 3 - Review of Passive NFEs that have accounts over USD 1 million[79] at the occasion of asking for self-certification from those passive NFEs

This option would provide a one-off review of the business relationship with regard to the beneficial ownership of existing customers that are Passive NFEs (like trusts, other legal arrangements and legal entities such as foundations, or other passive structures) and at the same time relying on synergies with the Directive on Administrative Cooperation.

The occasion of contacting the customer for obtaining a self-certification under the customer due diligence foreseen in the Directive on Administrative Cooperation would, under this option, prompt the financial institution to upgrade the beneficial ownership information under the 4 AMLD.

Since the performing of customer due diligence under the Directive on Administrative Cooperation will take place for two years between 2016-2017, this action should be considered as a priority in terms of timing.

Enhancement of the AML and transparency legislation

This option would increase the monitoring requirement on the beneficial ownership information for a subset of customers by reviewing the existing accounts of Passive NFEs together with the self-certification obtained under the Directive on Administrative Cooperation. This would significantly improve the EU transparency standards set in the Directive on Administrative Cooperation and the scope of the exchange with regard to Controlling Persons of Passive NFEs.

[79] The self-certification for Pre-existing Accounts of Passive NFEs applies to accounts above USD 1 million.

Costs and administrative burden

The process of contacting and reviewing existing customers under 4AMLD would be facilitated since it would be possible to carry out that process in parallel with due diligence under Directive on Administrative Cooperation which has already started. The additional administrative burden would be minimal due to the outlined mutual synergies from the parallel operation of the customer due diligence under the Directive on Administrative Cooperation and the 4 AMLD. The existing process for contacting the customer and obtaining information is already well-established by financial institutions. In terms of practical implementation, Financial Institutions may even extend the self-certification to include fields on beneficial ownership information in accordance with the 4AMLD.

Data protection and fundamental rights

Smaller additional set of data of beneficial owners would be affected. The data include identification and details on settlors and beneficiaries only of trusts that are Passive Non-Financial Entities that hold financial accounts with a balance or value over USD 1 million with financial institutions. That information could be used to fight money laundering, but is specifically targeted for tackling the problem of tax evasion by way of automatic exchange of information.

Proportionality

This option meets the proportionality test due to the possibility of using the self-certification process in the Administrative Cooperation Directive as an avenue to request, in addition, an update of the beneficial ownership information, while targeting only high-value accounts of entities that function as passive intermediary structures.

5.1.1.4. Summary Comparison of options

Objectives/impacts	**Option 1** Baseline	**Option 2** Review of all existing customer relations	**Option 3** Review of Passive NFEs that are subject to self-certification	Comments
Enhancement of the AML and transparency legislation	0	+++	++	The option of a systematic review has the most impact in terms of enhanced beneficial ownership information. The option limited only to high-value entity accounts of passive non-financial entities is more targeted and would also be a clear improvement.
Costs/Admin burden	0	---	-	The administrative burden associated with asking for an update by all obliged entities for all their customers is significant. In contrast, the option limited only to high-value entity accounts of passive non-financial entities would involve minimal additional cost, since the process of contacting the customer would already be set up for the purpose of obtaining self-certifications.
Data protection/ fundamental rights	0	--	-	The collection of more information under the option of a systematic review is at least as favourable in terms of data protection.
Proportionality	N/A	-	+	The approach of targeting only entities that are passive non-financial entities and have high-value accounts (>$1mln) is much more proportionate than the option of a systematic review.

Conclusions	0	-	++	While the option limited only to high-value entity accounts of passive non-financial entities will have lower impact on transparency and beneficial ownership, it is much more proportionate and is associated with a significantly lower administrative burden.

Option 3 is recommended as the most effective and proportionate solution

5.1.2. The ownership threshold of 25% applies both to genuine commercial corporate entities, and intermediary structures that adopt a corporate form

5.1.2.1 Problem Definition

Like trusts, offshore corporate entities are often used to distance the beneficial owner from the assets for various reasons and often for tax evasion. The EU and global instruments to tackle this issue are respectively the Directive on Administrative Cooperation and the Global Standard on Automatic Exchange of Financial Account Information. These instruments rely extensively on information collected for AML purposes.

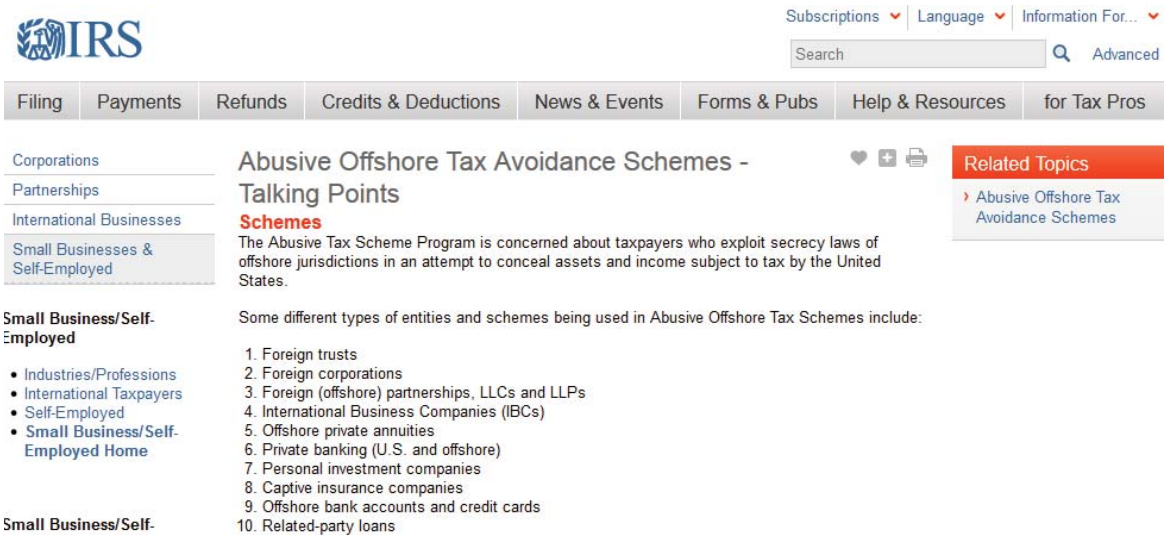
The beneficial ownership threshold in the 4 AMLD does not distinguish between genuine commercial corporate entities and those that have no active business and are mostly used as an intermediary structure between the assets/income and the real beneficial owner. For the latter, the 25% threshold is very easy to circumvent, leading to no identification of these beneficial owners and therefore a possibility to circumvent EU and global transparency standards.

Figures on dimension - prevalence of offshore intermediary entities

Evidence on the prevalence of offshore intermediary entities put forward in section 2.1.1. is applicable to intermediary entities that adopt a corporate form. As stated there, the legal form used largely depends on the legal framework under which entities are usually created in a specific jurisdiction. For example, the intermediary entities that Mossack Fonseca was creating in **Panama** (almost **50.000**) had a corporate form. Therefore, it can be assumed that the Panama intermediary entities that hold 20% of Swiss fiduciary deposits have a corporate form.

Notably the US Internal Revenue Service lists "Foreign corporations" right next to "Foreign trusts" as entities that are being used in abusive offshore tax schemes[80].

[80] https://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Abusive-Offshore-Tax-Avoidance-Schemes-Talking-Points



IRS

Subscriptions | Language | Information For...

Search Advanced

Filing | Payments | Refunds | Credits & Deductions | News & Events | Forms & Pubs | Help & Resources | for Tax Pros

Corporations
Partnerships
International Businesses
Small Businesses & Self-Employed

Small Business/Self-Employed

- Industries/Professions
- International Taxpayers
- Self-Employed
- Small Business/Self-Employed Home

Small Business/Self-

Abusive Offshore Tax Avoidance Schemes - Talking Points

Schemes

The Abusive Tax Scheme Program is concerned about taxpayers who exploit secrecy laws of offshore jurisdictions in an attempt to conceal assets and income subject to tax by the United States.

Some different types of entities and schemes being used in Abusive Offshore Tax Schemes include:

1. Foreign trusts
2. Foreign corporations
3. Foreign (offshore) partnerships, LLCs and LLPs
4. International Business Companies (IBCs)
5. Offshore private annuities
6. Private banking (U.S. and offshore)
7. Personal investment companies
8. Captive insurance companies
9. Offshore bank accounts and credit cards
10. Related-party loans

Related Topics

› Abusive Offshore Tax Avoidance Schemes

Having been aware of such circumvention techniques, the United States included a 10% ownership threshold in considering a substantial US owner for the purposes of the automatic exchange of information under the Foreign Account Tax Compliance Act (FATCA). This provision applies as of 1 July 2015.The final FATCA regulations state the following:

(2) SUBSTANTIAL UNITED STATES OWNER

(A) In general The term "substantial United States owner" means—

(i) with respect to any corporation, any specified United States person which owns, directly or indirectly, more than 10 percent of the stock of such corporation (by vote or value),

(ii) with respect to any partnership, any specified United States person which owns, directly or indirectly, more than 10 percent of the profits interests or capital interests in such partnership, and

5.1.2.2. Problem drivers

Article 3(6)(a) of the 4 AMLD determines the criteria that shall be taken into account to identify the beneficial owner of corporate entities. One of these criteria, while only considered as an indication, is a threshold shareholding of 25% plus one share or an ownership interest of more than 25%.

While that threshold may be considered suitable for corporate entities that have commercial activities, this might not be the case for intermediary entities that are set up in the form of a legal entity, but in practice may function similarly to trusts in distancing the beneficial owners from the assets.

For those entities, the 25% threshold is fairly easy to circumvent, leading to obscuring of their beneficial ownership. By contrast, trusts and similar legal arrangements that, as outlined in section 2.1.1, are often used as similar passive structures, are subject to much more rigorous identification of the settlor, trustee, beneficiaries, etc., without any threshold for their share in the trust's assets.

The objective is to increase the scope of beneficial ownership of intermediary structures that have a corporate form.

5.1.2.3. Regulatory options

Option 1 - Baseline scenario - no action

No action would lead to the continued potential circumvention of existing EU transparency standards found in the Directive on Administrative Cooperation and an opportunity to hide illicit money.

Option 2 - Reduction of the ownership threshold for all corporate entities

One option could be to reduce the 25% ownership threshold for all corporate entities in order to address cases where these are set up in ways to circumvent the threshold.

Enhancement of the AML and transparency legislation

This option would increase the scope of all beneficial ownership information for all corporate entities, which may reveal important beneficial owners with ownership lower than 25%. This option does not rely on a distinction between the types of entities and to that extent would meet the objective with greater certainty. For example, under the Directive on Administrative Cooperation, all newly set up NFEs are not considered Passive in the first two years after their creation.

Costs and administrative burden

The associated administrative burden of lowering the threshold across the board may be significant. The new requirement would need to be applied by all obliged entities that are financial institutions under the Directive on Administrative Cooperation for their customer due diligence on all new customers, and for existing customers the impact would depend on what option for existing customers monitoring is chosen in the previous section.

Data protection and fundamental rights

A larger set of beneficial owners would be detected. The data include identification and details on all owners having ownership that exceeds 10% in any corporate entity. That information would be used to fight money laundering, but it would also be the basis for tackling the problem of tax evasion by way of automatic exchange of information.

Proportionality

While this option would enable important beneficial owners to be revealed, it entails a high cost of implementation, since it will also impact genuine commercial businesses and would imply a change in the customer due diligence for almost all clients of all obliged entities. As such, this does not seem proportionate in comparison to the envisaged objective.

Option 3 - Additional 10%[81] beneficial ownership threshold for Passive Non-Financial Entities

Under this option, a lower threshold would only apply to non-financial entities which do not engage in an active business activity (i.e. which limits the scope of entities on which the obliged entities would need to collect additional information to those where the risk of use for illicit purposes is very high). Accordingly, the reduced scope would only affect Passive Non-Financial Entities that are a subset of all Reportable Entities, which are in turn a subset of all Account Holders. The distinction between Active and Passive Non-Financial Entities is already foreseen in the Directive on Administrative Cooperation.

Enhancement of the AML and transparency legislation

[81] The 10% threshold is a desirable and proportionate figure that would make devising schemes around it more difficult. It reflects the threshold under FATCA.

Such a reduction of the threshold would enable the detection of beneficial owners with particular focus on entities that function as intermediary structures, do not create income on their own, but mostly channel income from other sources (Passive Non-Financial Entities under Directive 2011/16/EU – DAC2).

Since both trusts and corporate entities are used for offshore tax evasion, the proposed action will work towards aligning the scope of beneficial owners of trusts, where there is no ownership threshold, with the scope of beneficial owners of the specific type of corporate entities that are considered as Passive NFEs. This is also an improvement in terms of level playing field between those entities.

Costs and administrative burden

In order to reduce the potential administrative burden, the suggested approach again relies on synergies with the customer due diligence under the Directive on Administrative Cooperation and does not impact ordinary commercial businesses. The identification of those entities must be undertaken in any event under the revised Directive on Administrative Cooperation, so the actual additional burden for the obliged entities would be restricted to the identification of the beneficial owners of Passive Non-Financial Entities which have ownership between 10% and 25% (since above the 25% threshold there is already such an obligation). Therefore, there is no additional burden for the financial institution in distinguishing between Passive and Active Non-financial Entities, since that financial institution should already have performed its analysis under the Directive in Administrative Cooperation.

The additional burden is in identifying the additional beneficial owners who have ownership between 10% and 25% and performing the customer due diligence. Since the full set of information on Entity Accounts will be finalised by end-2017, it is currently impossible to determine the number of Passive Non-Financial Entities. There is also no indication on the number of beneficial owners who have ownership of such corporate entities between 10% and 25%.

Data protection and fundamental rights

Smaller additional set of beneficial owners would be detected. The data include identification and details on all owners having ownership that exceeds 10% in a Passive Non-Financial Entity. That information could be used to fight money laundering, but is specifically targeted for tackling the problem of tax evasion by way of automatic exchange of information.

Proportionality

This option meets the proportionality test, because it would apply only to a subset of all entities that bear the highest risk of being used as intermediary structures. That subset is already clearly identified in the Directive on Administrative Cooperation and the Reporting Financial Institutions have already implemented processes to cater for the distinction between passive and active entities.

5.1.2.4. Comparison of options

Objectives/impacts	**Option 1** Baseline	**Option 2** Reduction of the threshold for all corporate entities	**Option 3** Additional beneficial ownership threshold for Passive Non-Financial Entities	Comments
Enhancement of the	0	+++	++	The option of reduction of the

AML and transparency legislation				threshold for all entities is the most impactful in terms of greater transparency. The option limited only to passive non-financial entities is more targeted and would also be a clear improvement.
Costs/Admin burden	0	---	-	The administrative burden associated with applying a lower beneficial ownership threshold is much higher than applying that threshold only for passive non-financial entities.
Data protection/fundamental rights	0	--	-	The collection of more information under the option of general lowering of the beneficial ownership threshold is least favourable in terms of data protection.
Proportionality	N/A	-	+	The approach of a lower beneficial ownership threshold only for entities that are passive non-financial entities is much more proportionate than the option of a general lower beneficial ownership threshold for all corporate entities.
Conclusion	0	-	++	The lower beneficial ownership threshold only for passive non-financial entities will have lower impact on transparency and beneficial ownership and is much more proportionate and associated with a lower administrative burden.

Option 3 is recommended as the most effective and proportionate solution.

5. 2. Publicity of the beneficial ownership registers for legal entities

Context

In many countries around the world it is not a legal requirement to publish the name of a company. This way creating “anonymous companies” allow for the hiding of cash.

Anonymous companies and different types of legal arrangements often have very few or no employees at all, and most do not conduct any real business.

Research and law enforcement investigations demonstrate the link between the abuse of legal entities and arrangements, on the one hand, and, on the other hand, terrorist financing, money laundering, tax evasion and avoidance, and other forms of serious criminal activity.

The 4AMLD already establishes obligations in respect of the identification of the beneficial owners of legal entities and legal arrangements. The beneficial owner is defined by the Directive as "any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted" by reference to the customers of the obliged entities.

The revised standards adopted by the FATF in 2012 have put a specific emphasis on the prevention of legal persons or legal arrangements from being misused for money laundering or terrorist financing purposes. Following these standards, countries shall ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons and legal arrangements that can be obtained or accessed in a timely fashion by

competent authorities or by obliged entities when they need to undertake their customer due diligence measures.

5.2.1. Public access to the beneficial ownership registers for legal entities (such as companies)

5.2.1.1. Problem definition

The 4 AMLD has put in place strong provisions to enhance transparency requirements on beneficial ownership information.

According to the FATF standards, the determination of a beneficial owner of a company can be based at least on basic information which includes, at a minimum, the legal ownership and control structure of the company (status, powers, shareholders and directors of the company). These standards also provide some recommendations concerning possible mechanisms and sources that could be used for obtaining beneficial ownership information of legal persons (such as company registers, information held by the company itself, reliance on existing information…) but without giving preference for one system over another.

Taking into account the new focus on transparency and the need for tracing criminals who might otherwise hide their identity behind a corporate structure, Article 30 of the 4AMLD follows FATF standards and requires Member States to ensure that entities incorporated within their territory obtain and hold adequate, accurate and current information on their beneficial ownership. However, the 4AMLD goes further than the FATF standards in terms of enhanced transparency in order to combat the misuse of legal entities through two specific elements:

(i) A storage requirement: Article 30.3 requires from Member States to ensure that the information on beneficial ownership of corporate and other legal entities incorporated within their territory, including details of the beneficial interests, is stored in a central register located outside the company. The Directive leaves to Member States the possibility to use already existing systems to organise the storage of the beneficial ownership information, referring to a central register "for example a commercial register, companies registers as referred to in Article 3 of the Directive 2009/101/EC, or a public register".

(ii) A specific access mechanism: Article 30.5 requires from Member States to ensure that the information is accessible in all cases to competent authorities and Financial Intelligence Units (FIUs) without any restriction; to obliged entities in the framework of their customer due diligence obligations; and to any person or organisation than can demonstrate a legitimate interest. The definition of the legitimate interest notion is left to national appreciation..

Following Article 30.5 § 2, the basic information on the beneficial owner of a company shall at least include the name, the month and year of birth, the nationality and country of residence of the beneficial owner, as well as the nature and extent of the beneficial interest held (i.e. number of shares, voting rights, nature of the control – direct or indirect).

While these recent amendments present a major step forward in the prevention against money laundering and terrorist financing, the Panama's Papers' findings reveal the need to assess access to information notwithstanding the fact that the transposition of the Directive is still ongoing.

5.2 1.2. Problem drivers

Article 30 of the 4 AMLD requires that beneficial ownership registers are accessible by different actors with different levels of access and introduces, in particular, the concept of "legitimate interest" for other persons than authorities and obliged entities. This concept aims at addressing potential data protection and privacy concerns and has to be defined and assessed at national level. However, this criterion related to the legitimate interest left to national discretion may lead to excessive limitations of the access to the register as well as to a lack of a level playing field. The Directive also leaves the possibility to Member States to establish a fully public register (although this is only optional).

The timely access to beneficial ownership information may be hindered by this complex mechanism of differentiated levels of access and may create some discrepancies from one Member State to another.

In addition, these registers need only to be accessible to competent authorities, FIUs, obliged entities, and "persons who can demonstrate a legitimate interest to access the information", and not the wider public.

Members of the G8 leading global economies committed to keeping beneficial ownership registers already back in June 2013, and the UK confirmed that it would make its register publicly accessible that November. Implementation of these commitments is being overseen by the global standards-setting body the FATF.

5.2.1.3. Regulatory options

Option 1: Baseline scenario

No action would lead to keep the differentiated levels of access as they are currently provided under the 4 AMLD, allowing competent authorities, FIUs, obliged entities and any other persons who have a legitimate interest to have access to the relevant beneficial ownership information.

Option 2: to make the current optional system in the 4AMLD mandatory, by giving full public access rights to the information held in beneficial ownership registers of legal entities.

Data protection and fundamental rights

The option concerning the full public access to beneficial ownership information have to be looked into taking into account the proportionality and possible impacts on the protection of personal data and the right to privacy. It is worth recalling that the Commission made a public statement related to access by any other persons having a legitimate interest. The Commission underlined in particular that, when transposing the Directive, Member States will need to pay particular attention to such requirements in order to ensure that the access of third parties pursues an objective of general interest and that the necessity and proportionality which would justify the potential restrictions of the protection of personal data and the right to privacy are fully established[82].

Hence, full public access needs to be carefully assessed regarding its compatibility with the Charter.

In addition, Article 30.9 provides that exemptions from giving access to the register to obliged entities and any other person can be allowed on a case-by-case basis in exceptional

[82] Declaration by the Commission in COREPER January 2015

circumstances, in particular where such access would expose the beneficial owner to the risk of fraud, kidnapping, blackmail, violence or intimidation. This mechanism may be kept in the proposed revision of the Directive as a safeguard in order to ensure that the purpose limitation is respected and sensitive information related to the beneficial owner is not misused for other purposes than those strictly defined by the Directive, i.e. the fight against money laundering and terrorist financing.

Given all these caveats, conditions under which access to information on beneficial ownership is granted would need to be wholly redefined. Public access to beneficial ownership information aims primarily to ensure enhanced corporate transparency, and clear rules – while allowing greater scrutiny of information by civil society – would primarily benefit anyone wishing to do business with a company/legal entity. Therefore, the new rules would need to be implemented by compulsory disclosure of certain information on the beneficial ownership through the registers set up in accordance with the 1st Company Law Directive (Directive 2009/101/EC[83]), the Union legal act that lays down the rules on disclosure of company documents and the validity of obligations entered into by a company.

Administrative burden

Opening a fully public access for beneficial ownership registers for companies would not have additional impacts on the market in term of administrative burden as there is already an existing obligation under Article 30.3 of the Directive to collect the relevant information and included it in the register for all entities concerned (i.e. corporate and other legal entities incorporated within the territory of a Member State).

Costs

Opening a fully public access to beneficial ownership registers of companies would have a positive impact from the point of view of costs and IT resources as it will bring a simplification in the modalities of access to the information held in the registers by dispensing of the current obligation to put in place complex layers of access. In this respect, Member States have already raised, during the transposition workshops organised by the Commission, some concerns about the concrete implementation of Article 30, in particular:

- on how to concretely define the notion of legitimate interest (Article 30.5 c): some Member States have difficulties in defining categories of persons and organizations that are able to demonstrate they have legitimate interest with respect to money laundering and terrorist financing, and the associated predicate offences (corruption, tax crimes and fraud);
- on whether the access to the national beneficial owners' registers by obliged entities from another Member is allowed (Article 30.5 b));
- on why a Financial Intelligence Unit of one Member State cannot access directly the national register of another Member State and should instead ask its own FIU to do so (Article 30.6).

By opening fully the register, the access would be easier and less complex to organise.

Effectiveness

[83] Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).

Giving full public access rights to the information held in the registers will ensure more consistency in the EU framework as regards the access to beneficial ownership information and more efficiency in the traceability of the beneficial owner.

Currently, the practices are really different from one Member State to another, and there is sometimes confusion between legal ownership and beneficial ownership information which can be clarified by giving full access to a complete set of information related to a company structure.

From sources we collected in different reports and existing legal requirements it appears that:

(i) in relation to limited liability companies, business registers in the Member States hold and disclose not only basic information on the company (name, registered office, articles of association and registration number), but other details as well, such as names of legal representatives, and names of directors or members of supervisory boards (Article 2 of Directive 2009/101/EC).

(ii) concerning company shareholders, there was – until the 4AMLD - no EU-wide requirement to disclose such information in the register. However, a number of Member States hold data on shareholders and even on the extent of shareholding. According to the 2014 report of the European Commercial Registers' Forum (ECRF) at least 10 EU businesses registers store shareholders' data and make it available to the public.

(iii) in respect to beneficial ownership information, there is little information available on existing practices in the Member States related to beneficial ownership data (given that the 4AMLD is not yet transposed). The 2014 ECRF report indicates that the business registers from Croatia, Italy and Latvia are already responsible for registering beneficial ownership information. In Luxembourg, an authority other than the business register has this responsibility. In Italy, Latvia and Luxembourg, beneficial ownership details are currently not made available to the public, but only to specific public authorities. Estonia, Romania and Slovenia also hold information on beneficial owners and make it available to the public.

(iv) according to the Bownet report published in February 2013[84], ownership structures and identification of beneficial owners rely mainly on information about company shareholders and board members and managers. Concerning access to data which allows for identification of beneficial ownership, the same report shows that even when the names of shareholders are made available to the public, other details such as home address or birth date (which can be very important for dealing with cases of homonymy) are only disclosed to certain competent authorities. Similarly, while names of directors are stored by the registers, it is not always the case that all details on directors are disclosed to the public. Information on home address, date of birth, personal ID/passport number is often made available only to certain authorities.

5.2.1.4. Comparison of options

Objectives/impacts	**Option 1** Baseline	**Option 2** mandatory full public access rights to the	Comments

[84] Bownet is a European Commission funded project which looked specifically into the issue of identifying the beneficial owner of legal entities in the fight against money laundering : http://www.transcrime.it/wp-content/uploads/2013/11/BOWNET3.pdf

		info held in BO ownership registers of legal entities	
Enhancement of the AML and transparency legislation	0	++	Option 2 would: - facilitate FIU's direct access to a national register of another MS (FIU-to-FIU request not required). - due to simplification (see admin below) make it easier (faster) for MS to get registers up and running; and - facilitate the interconnection of registers as all MS will have the same public access model/rules for access.
Costs/Admin burden	0	++	Option 2 would: - bring simplification by having one simple modality of access to BI info, as legitimate interest must no longer be demonstrated. It would also facilitate cross border requests (as mentioned above); and - not have additional impacts on the market in term of administrative burden as there is already an existing obligation to collect the relevant information and included it in the register for all such entities
Data protection/fundamental rights	0	--	AMLD already gives limited public access to BO information (if a "legitimate interest" is demonstrated) but there are legal risks in terms of compatibility with the Charter of Fundamental Rights and further analysis is required.
Proportionality	0	--	There is a valid public interest objective but the effect on and compatibility with the Charter of Fundamental Rights must be assessed before a proportionality assessment is completed (i.e. if it goes beyond what is necessary to prevent ML and the effect on other public interest objectives)

5.3. Trusts are not sufficiently transparent

5.3.1. Registration of trusts - territorial dimension and scope

5.3.1.1. Problem definition

Beyond the issue of the identification of the beneficial owner of a trust (see point 5.1.1), there is a need to clarify the exact features of the registration requirements. This clarification is needed for the following reasons:

Territorial dimension

The current provisions in the 4AMLD state that Member States shall require trusts governed under their law to obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust (Article 31.1 of the 4AMLD). In addition, when trusts open accounts with financial institutions in the EU, the financial institutions must collect that information from the trust. Under the Directive on Administrative Cooperation in certain cases this beneficial ownership information, together with other financial and tax information, must be passed to the financial institution's tax authority that then transfers this where

appropriate to other Member States' tax authorities. In addition, that information on the beneficial ownership of trusts which generate tax consequences must be included in a trust register.

However, there are some problems with the application by Member States of the first step, since those provisions are not unequivocally or consistently understood and applied by Member States. Some Member States do not consider trusts set up under another Member State's law (common law) to fall within their jurisdiction even if they are administered in their territory because they do not recognise such legal structures. At the same time, common law Member States do not consider trusts set up under their own law to fall within their jurisdiction unless they are administered in their Member State.

This risks creating gaps that certain trusts might remain unmonitored by any Member State. Those trusts would also not be obliged to register. When such a trust opens an account with an EU financial institution, the institution will collect the relevant information and pass it on to the tax authorities under the Directive on Administrative Cooperation, but there is no Member State checking/monitoring whether the trust beneficial ownership information is correct. In addition, the bank is not able to check in the trust register.

Scope of registration

A second problem arises because the requirement under the 4AMLD for trusts to be registered in national registers only applies where they 'generate tax consequences'. If a trust does not generate 'tax consequences', the Directive does not impose any registration requirement of this one.

There will be no check on a trust registration as it is not registered anywhere, and no way for a financial institution to cross check details with the register. Although the trust will have to provide the information on an account, and the information may pass under the Directive on Administrative Cooperation as appropriate, there is another potential weakness in the controls and checks.

Therefore, this limitation of the registration requirement only to trusts which generate tax consequences is not fully consistent with the overall obligation under the 4AMLD to identify, in the course of performing customer due diligence on the customer, the involvement of any type of trust and the relevant information pertaining to it before entering into a business relationship.

Figures on dimension

It is not practically possible at this time to obtain figures on the number of trusts active in the EU, or the assets held through those entities. Nevertheless, the evidence provided in section 5 on the way in which certain types of trusts achieve effective distancing of the original contributor (settlor) and beneficiaries from the trust's assets is relevant for trusts operating within the EU implying that there are trusts holding significant amount of assets.

5.3.1.2. Problem drivers

Article 31 of the 4AMLD imposes the following obligations on Member States:

(i) to require that trusts *governed under their law* obtain and hold adequate, accurate and up-to-date information in particular on the trustee;

In terms of application of this requirement, some Member States tend to consider, based on the current text of Article 31, that as long as they do not recognise trusts in their law, they are not submitted to any obligation of registration of trusts administered in their territory[85].

This risks creating gaps and is not in line with the objectives of the transparency requirements of the Directive, which should therefore be amended to clarify the current understanding that the Member State where the trust is administered (i.e. through the trustee by opening an account, undertaking a real estate transaction or investment, etc.) shall be responsible to register the trust[86].

(ii) to put in place, at national level, *centralized registers of beneficial owners* of trusts which *generate tax consequences* and to give access to the information to the obliged entities (banks, financial institutions, legal professionals, real estate agents, etc.), competent authorities and financial intelligence units.

[85] This statement has been made during the workshops organised by the Commission in the context of the transposition of the 4AMLD.

[86] This approach would be consistent with paragraph 62 of the FATF's Guidance on Transparency And Beneficial Ownership.

The registration requirement is currently imposed only as regards trusts which *generate tax consequences*. The registry is supposed to be a tool to help competent authorities, financial intelligence units and obliged entities to gather relevant information on beneficial ownership of trusts. This limitation of the registration requirement only to trusts which generate tax consequences is not fully consistent with the more encompassing obligation under the Directive to identify all types of trusts before entering into a business relationship.

The result is also inconsistent in the sense that the current registration requirement exempts from registration trusts that, whether intentionally or unintentionally, and due to mismatches in the legal and tax systems, fall outside the scope of the taxation rules of Member States (e.g. due to having no tax residence anywhere). Therefore, such trusts would enjoy not only being exempt from having to pay taxes, but in addition to that, would not be registered anywhere. That combination puts those types of trusts into a category of high risk for tax evasion and hiding illicit money.

The objective is to ensure that all trusts that are operating in the EU are properly monitored and registered in the EU.

(iii) Competent authorities and financial intelligence units are supposed to provide information on the beneficial owner of a trust to the competent authorities and to the financial intelligence units of other Member States in a timely manner. As the trust (being largely a common law entity) and the trustee (who can operate in any jurisdiction) may not depend on the same territorial competence, there is an interest in ensuring a smooth process of communication between competent authorities on that matter.

5.3.1.3. Regulatory options

Option 1 - Baseline scenario - no action

No action would lead to continued ambiguity in the registration requirements of trusts, in parallel with increased risk of the use of some trusts as vehicles for tax evasion.

Option 2 - Registration of all trusts according to the law under which they are set up

This option would involve:

- monitoring of trusts by the Member State under the laws of which the trust is set up, regardless of any financial activities in that Member State
- registration also in the Member State under the laws of which the trust is set up
- extending the scope of the registration requirements to all trusts, and not only to those which “generate tax consequences”.

Enhancement of the AML and transparency legislation

The wider scope of registration for all trusts will enhance the transparency requirements of the 4 AMLD, meeting the objective of ensuring that all trusts that are operating in the EU are registered in the EU. Nevertheless, such a formal requirement may not be very effective in practice, since the absence of financial activities of any of the actors related to the trust in the Member State under the law of which the trust is set up (typically, a common law country) may make it difficult for that Member State to identify the trust and even more difficult to register and monitor it in the future. That would also be inconsistent with the FATF Recommendations.

Costs and administrative burden

There is additional administrative burden associated with the extension of the scope of the registration requirements to all trusts. This additional administrative burden for the trustee is higher than in Option 3, due to the need for the trustee to maintain connection with a Member State that he does not operate in but under the law of which the trust is set up.

This would also bring significant burden to those Member States which have common law legal systems governing trusts. While they have concepts and principles in place to deal with such structures domestically, they have no means to know how many trusts are constituted and operate in other countries.

Data protection and fundamental rights

This option would entail an increased scope of the information on trusts and their beneficial owners in national registers. The information includes identification and details on beneficial owners of all types of trusts. That information would be used to fight money laundering, but it would also be the basis for tackling the problem of tax evasion by way of automatic exchange of information.

Proportionality

As outlined, this option is potentially not very effective and is associated with higher administrative costs for both the Member States and the entities concerned. Therefore, this option is not favoured in terms of proportionality.

Option 3 - Registration of all trusts according to the place of administration of the trust

This option would involve:

- monitoring of trusts in the Member State where the trustee operates/administers the trust
- registration also where the trustee operates/administers the trust, irrespective of whether the Member State in question regulates or indeed recognises such legal structures in its national law.
- additional one-off notification to the Member State under the law of which the trust is governed
- extending the scope of the registration requirements to all trusts, and not only to those which "generate tax consequences"

The proposed functioning of the system is best illustrated with the following hypothetical example:

A trust is set up under the law of Member State A but is administered by a trustee in Member State B and has only Member State B's beneficiaries. The trust is not considered to be resident in Member State A, but is also not a separate taxable person in Member State B. Even though the trust does not "generate tax consequences" in either of those two Member States, it would have to be monitored by Member State B's competent authorities. Furthermore, the trustee would have the obligation to register with the Member State B trust register.

Separately, given that the Member State of administration (Member State B) has to deal with legal arrangements that are foreign to its legal system and in order to facilitate the registration, this option foresees a one-off notification by the trustee to the Member State under the law of which the trust is governed (Member State A). That notification may include information on the setting up of that trust, its trustee and place of administration. That Member State A and

the Member State B where the trustee operates/administers the trust should cooperate in order to ensure the effective registration of the trust in the latter Member State.

Enhancement of the AML and transparency legislation

The wider scope of registration for all trusts would give more consistency to the EU framework as the transparency requirement would apply to the beneficial owners of all types of trusts, which even now have to be identified by the obliged entities under their customer due diligence obligations, regardless whether they generate tax consequences or not. Therefore, this approach is an improvement in terms of enhancement of the AML and transparency legislation as it meets the objective of ensuring that all trusts that are operating in the EU are properly monitored and registered in the EU.

In terms of the territorial dimension of the monitoring and registration requirement, this option would mean that the monitoring and registration requirement applies to all Member States, including those who have no provisions on trusts in their national framework. At the same time, it creates a level playing field by confirming that common law Member States will not be the only Member States responsible for taking care of this registration requirement. In addition, that approach would align very closely the connecting factor for Investment Entities that are trusts under the Directive on Administrative Cooperation with the registration under the 4 AMLD. In particular, where a trust is an Investment Entity under the Directive on Administrative Cooperation, it is considered as a Reporting Financial Institution in the Member State where the trustee is resident, with the assumption that this is the place where the trust is administered.

The cooperation among Member States enabled by the one-off notification to the Member State under the law of which the trust is governed brings additional certainty that the registration would be done with proper understanding by the Member States concerned of the legal aspects related to various types of trusts.

Costs and administrative burden

There is additional administrative burden associated with the extension of the scope of the registration requirements to all trusts. This additional administrative burden for the trustee is lower than in Option 2, due to the fact that the trustee would carry on his activities in administering the trust in the Member State where that trustee is registered. However, it is impossible to measure the scope of the impact due to the lack of data as to the approximate number of trusts and similar legal arrangements which will be concerned.

The one-off notification of the Member State under the laws of which the trust is set up (e.g. the United kingdom) would not be a significant additional administrative burden for the trustee, because it does not involve any continued correspondence or additional administrative steps in that Member State. The involvement of another Member State (the Member State under the laws of which the trust is set up) would increase the cost for that Member State's administration.

Data protection and fundamental rights

The information includes identification and details on beneficial owners of all types of trusts. That information would be used to fight money laundering, but it would also be the basis for tackling the problem of tax evasion by way of automatic exchange of information.

Proportionality

This option brings clarity to the territorial application of the provisions of the Directive. In the view of the Commission, Member States are already obliged to set up national registries of

trusts and to include the relevant information on the trustees and other actors concerned as long as the trust is administered in their territory. Thus, clarifying the state of play would not bring additional administrative costs. From the perspective of the trustee this is done at less expense for him than in Option 2 because s/he has to communicate with the competent authorities of the country in which s/he operates and not those of another Member State. Thus, this option also relies on cooperation among Member States' authorities in challenging cross-border scenarios. In this respect, this option meets the proportionality test because it ensures that all trusts that are operating in the EU are properly monitored and registered in the EU in the Member States to which they have the closest ties.

However, there are no figures available on how many trusts would be concerned by the registration requirement once the reference to "tax consequences" is removed and what the impact on them and on the register would be.

5.3.1.4. Comparison of options

Objectives/impacts	**Option 1** Baseline	**Option 2** Registration in jurisdiction of law	**Option 3** Registration in jurisdiction of administering	Comments
Enhancement of the AML and transparency legislation	0	++	+++	The registration in the Member State administering the trust with the notification to and subsequent assistance by the Member State of the law under which the trust was set up is practical and effective. Relying only on one or the other Member State alone has clear disadvantages in terms of efficiency.
Costs/Admin burden	0	--	-	The administrative burden associated with registration of all trusts is significant, but less so if that registration is with the Member State where the trust is administered.
Data protection/fundamental rights	0	--	-	The maintenance of trust registration in another Member State than the place of administration may pose further challenges.
Proportionality	0	-	+	It is clear that registration with the Member State of the law under which the trust was set up is inferior both in terms of effectiveness and associated costs.
Conclusion	0	--	+++	It is clear that the third option addresses the problem most adequately and at comparatively lower costs.

Option 3 is recommended as the most effective and proportionate solution

5.3.2. Public access to the beneficial ownership registers for legal arrangements (such as trusts)

5.3.2.1. State of play

According to FATF standards, the beneficial ownership information regarding a trust should include information on the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate control over the trust. As for companies, these standards also provide some recommendations concerning possible mechanisms and sources that could be used for obtaining beneficial ownership information of trust (such as registries or information held by competent authorities or by other agents and service providers to the trust), without, however, giving preference to one system over another.

Article 31 of the 4AMLD follows the FATF standards and imposes on Member states to ensure that trustees of any express trust governed under their law obtain and hold adequate, accurate and up-to-date information on beneficial ownership regarding the trust. The information shall include the identity of the settlor, the trustee(s), the protector (if any), the beneficiary or class of beneficiaries and any other natural person exercising effective control over the trust. However, the 4AMLD goes further than the FATF standards in terms of enhanced transparency in order to combat the misuse of legal arrangements such as trusts through two specific elements:

(i) A storage requirement: Article 31.4 requires from Member States to ensure that the information on beneficial ownership of trusts which generate tax consequences is stored in a central register.

(ii) A specific access mechanism: Article 31.4 requires from Member States to ensure that the information is timely and unrestrictedly accessible by competent authorities and Financial Intelligence Units. The register may also allow timely access by obliged entities, within the framework of customer due diligence.

5.3.2.2. Problem definition

As far as trusts are concerned, Article 31 of the 4AMLD requires that beneficial ownership registers are accessible by competent authorities, financial intelligence units and obliged entities in the same conditions as those provided for legal entities but not to third parties who have a legitimate interest. The main reason behind this limitation resides in the sensitiveness of trust information when dealing with non-professionally managed trusts (e.g. family trusts).

Any amendment to the current text needs to ensure a careful balancing of opposing legitimate interests. On the one hand, trusts are legitimate vehicles that offer a set of advantages, including preserving the assets of beneficiaries whose identity is protected. On the other hand, public interest in transparency would justify the disclosure of the beneficial owners of trusts.

5.3.2.3. Regulatory options

Option 1- Baseline scenario

No action would lead to keep the differentiated levels of access as they are currently provided under the 4 AMLD. Beneficial ownership information on trusts is supposed to be accessible without any restriction by competent authorities and FIUs, and in a timely manner by obliged entities within the framework of their customer due diligence requirements.

Option 2 - to give full public access to the beneficial ownership information on all trusts

Data protection

By removing the reference to "tax consequences", the scope of the trusts concerned by the publicity will be broader and the argument could be made that this risks touching on sensitive issues such as those relevant for family trusts. From a privacy point of view, this option is probably the most complex one. However, it can also be envisaged to replicate the provision which is currently provided under Article 30.9 of the 4AMLD for companies and which allows some exemptions from giving access to the register to obliged entities and any other person on a case-by-case basis in exceptional circumstances, in particular where such access would expose the beneficial owner to risk of fraud, kidnapping, blackmail, violence or intimidation. This mechanism may be introduced at least for "non-commercial/family" trusts in the proposed revision of the Directive as a safeguard in order to ensure that sensitive information related to the beneficial owner is not misused for other purposes that those strictly defined by the Directive, i.e. the fight against money laundering and terrorist financing.

Administrative burden

It is difficult to assess the administrative burden of the full public access for beneficial ownership registers for all trusts. However, practical implications can be assumed by the fact that the most important impact will be caused by the registration requirement which would be imposed to all trusts in advance in this hypothesis, namely as a result of the deletion of the "tax consequences" criterion. However, once the registration is completed, there is no evidence that the full public access will bring additional costs. For the same reasons as those exposed above, the public access will be practically easier to organise rather than differentiated levels of access which bring complexity.

Costs

As mentioned under the previous proposals above, opening a full public access for beneficial ownership registers for all trusts would have a positive impact from the point of view of costs and IT resources as it will simplify the modalities of access to the information held in the registers by dispensing of the current obligation to put in place complex layers of access.

Effectiveness

Giving full public access rights to the information held in the registers will ensure more consistency in the EU framework as regards the access to beneficial ownership information and more efficiency in the traceability of the beneficial owner of all trusts. However, from an anti-money laundering point of view, the efficiency of giving access to persons other than competent authorities to the information regarding the beneficial ownership of "family trusts" is not as straight forward (in terms of the potential risks of abuse) as for the other categories of legal entities and legal arrangements.

From sources we collected via open sources' information[87] it appears that the number of UK Family Trusts and estates required to complete a full self-assessment return was 168,000 in 2013-14. Total income reported by trusts in 2013-14 was £2,265 million (€2,878 million). Trusts paid a total of £1,210 million (€1,539 million) in taxes: £670 million (€852 million) in income tax and £540 million (€687 million) in capital gains tax. For tax purposes, a range of different categories of trusts are regarded collectively as 'UK Family Trusts'.

[87] Summary of HM Revenue and Customs statistical release of January 2016

5.3.2.4. Comparison of options

Objectives /impacts	Baseline scenario	Full public access to BO info held in BO registers relating to all trusts:
Enhancement of AML & transparency legislation	0	++
Cost effectiveness / Admin burden	0	++
Data protection / Fundamental rights	0	--
Proportionality	0	--

5.4. Certain public authorities lack information

5.4.1. Problem definition

The fact that Member States have the choice of whether to give certain access to information collected for the purposes of fighting money laundering and terrorism financing, and in particular beneficial ownership information to tax authorities, or not to give it to tax authorities (i.e. they are permitted to but they are not required to) in the 4 AMLD limits the effectiveness of tax audits as some tax authorities are currently not receiving the information. The information exchanged under the Global Standard and the Directive on Administrative Cooperation would trigger even more cases where such information would be critical in order to properly audit the compliance of Reporting Financial Institutions as defined in that Directive and taxpayers. To confirm if Financial Institutions are complying with their due diligence and reporting obligations, tax authorities will need access to information in particular on beneficial ownership, since the Directive on Administrative Cooperation builds on the assumption that the AML customer due diligence procedures are in place and are performed correctly. Law enforcement authorities may have similar interest in accessing certain information collected for AML purposes.

5.4.2. Problem drivers

The current drafting of the AMLD leaves it to national legislation to define the relevant competent authorities, but does not prohibit a Member State to include tax and law enforcement authorities in this group. National approaches at EU level vary significantly, with some EU Member States but not all already considering such authorities as competent authorities for AML purposes. Such a diverging position as regards access to beneficial ownership information by the tax authorities leads to an uneven playing field between EU Member States.

But the consequences go beyond a level playing field. The lack of access to such information hampers the activity and efficiency of the tax administrations themselves in their fight against tax avoidance, fraud and evasion. In practice, such a limitation constitutes an obstacle to their investigating powers, since information can be denied on the basis of the lack of competence – often such restriction translates into documents/information either being denied or, if

provided, where the relevant information is concealed under the argument that access to it cannot be granted.

Tax authorities already have information on the customer, through the company/legal persons registries in the various Member States, containing publicly available information. However, tax authorities need further information, for example on beneficial ownership. Only then will they be able to confirm that the information being provided under the existing legal instruments (not only at Union level, under the Directive on Administrative Cooperation, but also pursuant to a panoply of national legislation requiring the communication of information to the tax authorities) is accurate, as well as to confirm that the effective beneficial owners (and not nominees) are being reported and therefore subject to tax (and in some specific cases to international exchange between tax authorities for the same purpose).

While fulfilling their mission of fighting tax avoidance, fraud and evasion, tax authorities – even in the current context of limited access - play a key role in identifying other suspected serious crimes such as corruption, money laundering and terrorism financing. However, tax authorities are hindered in this role as they do not get a uniform access to the same information in all Member States, and even where some level of access is provided significant barriers, both of a legislative and non-legislative nature, remain.

5.4.3. Regulatory options

Option 1 - Baseline scenario – no action

In this scenario, the present situation, with all the limitations already explained, namely as regards the lack of a level playing field and the restriction of the activity of the national tax administrations, would remain.

Option 2 - Clarify in the text of the 4AMLD the notion of competent authorities.

This option would clarify which authorities may access information on beneficial ownership for the reasons already explained above.

Additionally, it would enable those authorities to correctly identify the beneficial owners of entities, legal arrangements and other, providing them with a key tool in the fight against tax avoidance, fraud and evasion, while having the necessary powers to verify that the information being provided to them under the various legal instruments available is accurate.

Costs and administrative burden

Access to beneficial ownership information does not imply a substantial additional cost or administrative burden for the following reason: the setting up of registries of beneficial ownership is already mandatory under the current provisions of the 4AMLD, and therefore this proposal would not add on this obligation, either for administrations or taxpayers. The only additional cost would be to make that same information available to the tax authorities, by providing access to tax authorities in a similar manner to which it is provided to the FIUs.

Data protection and fundamental rights

This option gives broader access to information to authorities other than AML authorities. The legitimate purpose of fighting tax evasion should be recognised as justifying such processing under the AML framework.

As a rule, tax administrations are already covered by secrecy requirements. Such access would fall into this scope and would be subject to the necessary safeguards.

5.4.4 Comparison of options

Objectives/impacts	**Option 1** Baseline	**Option 2** Clarification regarding access by tax authorities	**Comments**
Enhancement of the transparency	0	++	Option 2 would: - Provide for a level playing field within the EU for tax purposes; - Provide a key tool against tax fraud and evasion; - Enhance synergies between the action of the tax administrations and FIUs.
Costs/Admin burden	0	+	Option 2 would: - bring benefits as regards making the most of the available information, while - not have significant additional costs or administrative burden besides providing for the access by the tax authorities to information such as on beneficial ownership, since all the other aspects are already encompassed in the current framework.
Data protection/fundamental rights	0	0	The proposed change is a clarification of what is already allowed under the AMLD.
Proportionality	0	++	There is a valid public interest objective as regards the fight against tax fraud and evasion.
Conclusion	0	++	It is clear that the second option addresses the problem most adequately and provides for higher benefits.

Option 2 is recommended as the most effective and proportionate solution

6. MONITORING, TRANSPOSITION AND EVALUATION

As referred to in Part I of this Impact assessment (Section 9) Member States shall bring into force law, regulations and the administrative provisions necessary to comply with the 4AMLD and immediately communicate these texts to the Commission (Article 67 4AMLD).

Considering the fact that the transposition period of the 4AMLD is still ongoing, due care should be given to take into account as much as possible work already undertaken by the Member States when implementing and transposing obligations that are closely linked to the issues set forth in Part 2 of this impact assessment. In this respect, particular attention should be given to ensure continuity with the work already undertaken by the Member States regarding the creation of the registries/mechanisms mentioned in articles 30 and 31 of the 4AMLD.

According to article 65 of the 4AMLD, the Commission will conduct an evaluation of the extent to which this directive has been implemented in the Member States. By modifying the 4AMLD, this evaluation will also include the implementation of the measures that Member States have taken to achieve the general and specific objectives set out in this addendum.

The targeted modifications to the 4AMLD relating to Part 2 of this impact assessment can be monitored according to the following specific indicators:

Objectives	**Indicator**	**Source of info**
Improve the scheme of beneficial ownership information, by further enhancing transparency of (i) beneficial ownership information on corporate and other legal entities, and (ii) beneficial ownership information on trusts and other similar legal arrangements	- Type and characteristics of the instrument (registry/mechanism) put in place for the collection, storing and access to beneficial ownership information - Number and type of entities/legal arrangements for which beneficial ownership information is kept, and evolution of these figure over time - Number of Passive Non-Financial Entities for which beneficial ownership information is kept as from the 10% shareholding threshold (instead of 25%) - Type of information that is accessible to the different categories of persons having access to the registries/mechanisms - Frequency and triggers for updating existing information on the beneficial owners in the registries - Any problems linked to the creation and functioning of the abovementioned registers/mechanisms	- Member States
Improve access by public authorities and relevant stakeholders to beneficial ownership information	- Statistical data on the number of consultations of the registries/mechanisms by the different categories of public authorities, obliged entities and other persons that have accessed the registry during a defined period - Information on timeliness of access to the registries/mechanisms by public authorities, obliged entities and other persons that have access - Statistical information on the number and type of entities/legal arrangements for which beneficial ownership information was sought - Number of ML/TF files transmitted by FIUs to enforcement authorities, involving a prior consultation of the registries/mechanisms by obliged entities and AML/CFT competent authorities	- Member States - FIUs

Furthermore, the Commission will also work with the joint Committee of the European Supervisory Authorities on AML (AMLC) - which, amongst others produced reports on the implementation of the 3AMLD in some specific areas – in order to monitor the application of

the new legislative framework. The Expert Group on the Prevention of Money Laundering and Terrorist Financing (EGMLTF), could also serve as a forum for sharing information on application issues.

The 4AMLD allows Member States to adopt or retain in force stricter rules in the field covered by the directive (within the limits of EU law) and the Commission will pay particular attention to measures that are stricter that those presented in this Impact assessment.

At international level, monitoring of the application of the 4AMLD will also take place indirectly through the mutual evaluation processes of the FATF as well as Moneyval. This peer review process is an essential and rigorous process to ensure that Member States comply, both in law and in practice, with FATF international standards. The FATF is placing increased emphasis on the assessment of effectiveness of measures, as opposed to compliant legal frameworks. The mutual evaluations concerning individual EU Member States will represent an important element for the Commission's own evaluation of the effectiveness of the legal framework. In this respect it can be highlighted that good ratings in FATF or Moneyval mutual evaluation reports on EU Member States – including amongst other ratings on the specific standards relating to transparency of beneficial ownership information - would be indicators of the consistency of the EU approach with international standards and of the preservation of the EU financial system's reputation.

As regards the sources of information for the evaluation of any new measures - the Commission will collect additional data to assess and evaluate the efficiency of these measures.

ANNEXES

ANNEX 1: PROCEDURAL INFORMATION

Lead DG: Directorate General Justice and Consumers

Agenda Planning

Reference AP No	*Short title*	*Foreseen adoption*
2016/JUST+/054	*Directive amending the 4AMLD to strengthen the fight against terrorist financing*	*7/6/2016*

The improvement of the EU´s AML/CFT framework is part of the European Action Plan for strengthening the fight against terrorist financing adopted in February 2016. It also responds to the call for action by EU Finance Ministers at the informal ECOFIN Meeting in April 2016, to further improvements to the anti-money laundering framework.

The Commission decided to propose a number of targeted amendments to the 4AMLD at the latest by the end of the second quarter of 2016 on the following points addressed in **Part I**:

- enhanced due diligence measures/counter-measures to be taken towards high-risk third countries;
- virtual currency exchange platforms;
- prepaid instruments;
- enhance the powers of EU FIUs and facilitate their cooperation;
- provide the FIUs with swift access to information on the holders of bank-and payment accounts, through centralised registers or electronic data retrieval systems at national level.

As part of the European Agenda on Security, it belongs to the Commission's Work Programme 2016.

In view of the recent disclosures, by international media, that revealed significant deficiencies in the worldwide financial system and the informal ECOFIN Council's call for action, the Commission decided to add a number targeted amendments on the following points that are addressed in **Part II** to:

- keep the beneficial ownership/customer information up-to-date on an ongoing manner;
- lower the threshold for identifying the beneficial owner of entities covered by the directive;
- enhance access to beneficial ownership information;
- broaden the scope of registration of trusts;
- improve access to beneficial ownership information for legal arrangements (such as trusts); and
- allow for access to information on beneficial ownership by a broader set of competent authorities, in particular tax authorities.

Organisation and timing

An Inter-Service Steering Group (ISSG) was set up in February 2016. The ISSG is chaired by the Directorate General Justice and Consumers (JUST), and the following Services and Directorates General have been invited to participate: Secretariat-General (SG), Legal Service (LS), Budget (BUDG), Communication networks, content and Technology (CNECT), Economic and Financial Affairs (ECFIN), Financial Stability, Financial Services and Capital Markets Union (FISMA), Internal Market, Industry, Entrepreneurship and SMEs (GROW), Neighbourhood and Enlargement Negotiations (NEAR), Migration and Home Affairs (HOME), Taxation and Customs Union (TAXUD), Foreign Policy Instruments (FPI) and European External Action Service (EEAS).

The Inception Impact Assessment was validated by the First Vice Presidents cabinet on 21 March 2016 and published on 7 April 2016.

The ISSG met three times before the submission of the Impact Assessment to the Regulatory Scrutiny Board in April 2015. The ISSG approved the Impact Assessment on 8 April 2016 that was published on [tbc] 2016. The ISSG did not meet separately to discuss part II of this Impact assessment (sent to the Regulatory Scrutiny Board on 27 April 2016 as an addendum to the he Impact Assessment). Some of the issues in the addendum were raised at the final ISSG meeting that was held on 8 April, but, due to time constraints, ISSG members were instead consulted in a written procedure.

Consultation of the Regulatory Scrutiny Board

The Impact Assessment Report was examined by the Regulatory Scrutiny Board on 12 May 2016. In its positive opinion, the Board recommends that giving special attention to the following aspects:

Board's Recommendations	**Implementation of the recommendations into the revised IA Report**
1. Clarify the political context of the initiative: The report should better describe how the factual and political context has changed since the last revision of the Directive (4AMLD).	1. The Impact Assessment has been revised to better explained how the political context has changes since the adoption of the 4AMLD When revising the text particular attention has been given to clarifying how the recent terrorist attacks have led to the identification of problems that have not (or not sufficiently) been addressed under the 4AMLD, although some of these issue were discussed during negotiations. Also, the text has been clarified to highlight the links with other initiatives in the Action Plan to fight terrorism and terrorist financing, such as for example the FIU mapping exercise or the delegated act on high risk third countries. With regard to beneficial ownership issues, the report has been clarified on the recently changed context in this respect and the reasons why these policy options (such as for example providing for a mandatory access to the

	beneficial ownership registers for competent authorities) were not considered in previous revisions. The IA is also completed with a glossary, which has been added as a new annex 10 to make the text more accessible to the non-specialist reader.
2. Better explain the international context: Especially with regard to the beneficial ownership issues (addendum), the report should explain in how far the problem drivers are situated in the EU or in third countries and to which degree EU policy can address these problems.	2. The report has been updated to reflect how concerted strategies to obscure beneficial ownership information, often through the use of artificial structures located in third countries, have made it very difficult for the EU obliged entities to obtain such information (or easy for some entities to claim they could not obtain the information).
3. Better explain the EU added value of the proposed measures: The report should strengthen the subsidiarity analysis by showing how the functioning of the internal market could be affected if the identified problems were solely addressed at the national level. It should then explain why EU action would be more effective and efficient (explaining the advantages of a harmonised approach).	3. The report has been amended to strengthen the subsidiarity analysis by better explaining why the identified problems cannot be solved at national level or at international level (the FATF). The report also explains the adverse effect (creation of gaps and discrepancies which can be exploited by criminals and terrorists to channel their funds in and out the EU) that would be the result of a non-harmonized approach at EU level with regard to the identified issues. The report also puts forward the effects of a strongly integrated EU legislation in this field on the evolution of international standards. (effects on the standard-setting process at the FATF, etc…). The report also reflects the fact that if left to national initiative, the implementation of the measures would not be uniform throughout the EU, imposing different due diligence obligations and standards of knowledge on obliged entities which could lead to discrepancies and inefficiencies in the internal market.
4. Better explain the policy options and how they relate to each other.	4. The report clarifies how the various options for each problem differ from each other (e.g. prepaid instruments) or overlap/include each other (e.g. registers/mechanisms on bank and payment account holders). In case the preferred option is the result of a combination of multiple options, the need for this combination has been further explained (e.g. prepaid cards, virtual currencies). Also, on some issues, the report has further clarified the relation between certain regulatory options and discarded options or

	non-regulatory alternatives (e.g. FIU's access to – and exchange of – information). The interrelation and reinforcing effect of all the preferred options on the global AML/CFT process has also been further completed (cf. overview table on combined preferred options, clarifying the contribution of the preferred options on the different steps of the AML/CFT chain and global process as a whole).
5. Strengthen the impact analysis, particularly with regard to data protection issues: The impact analysis should assess whether the policy options are in line with and proportionate with regard to data protection issues (both for issues in the main text and in the addendum). It should specify which type of safeguards would need to be put in place for the various policy options in order to respect data protection rules. The impact analysis should also clarify why the additional administrative burden form the policy options remains limited (compared to previous revisions of the Directive). In the analysis, the diverging views of consulted stakeholder groups should be presented in more detail.	The report clarifies that the proposal concerns limited and targeted modifications to the recently adopted 4AMLD, and the fact that the current impact assessment builds upon the impact assessment of the 4AMLD for the general aspects (such as data protection and fundamental rights, quantification of costs and administrative burden, impacts on SME's, consumers, etc…), and therefore only focusses on additional impacts that could be generated by the proposed targeted amendments. On data protection, the preliminary remarks made by the EDPS on the issues contained in Part 1 have been integrated in the text, clarifying the additional safeguards needed in this respect.

ANNEX 2: STAKEHOLDER CONSULTATION

Brief summary of the consultation strategy/process

Due to the political urgencies and against the background that the envisaged amendments are targeted, it was considered that there was no needed to undertake an open public consultation. The proposed targeted amendments are presented in response to the Councils request to strengthen, harmonise and improve the existing and recently adopted EU legal framework to prevent the use of the financial system for the purposes of or terrorist financing and money laundering in specific areas.

Due to time constraints, the consultation strategy was based on a mix of targeted consultations (bilateral contacts, stakeholder- and experts meetings and written consultations), to complement the existing sources of information and provide additional data and facts and to provide the Commission with knowledgeable and representative opinions. The Commission has sought a wide and balanced range of views on this issue by giving the opportunity to a wide range of relevant parties (Member States, national authorities, the concerned private sector actors, consumer representatives, fundamental right stakeholders and data protection stakeholders) to express their opinions.

The consultations aimed at gathering targeted information to fill a limited number of information gaps that have been identified by the Commission's services following initial desk research based on preparatory work done in relation to the 4AMLD. Following this work, the Commission needed additional information and further data.

The Commission organised the following consultations throughout the impact assessment process:

I. Member States and national authorities:

a) Experts meeting with Member States representatives:

All EU Member States were consulted on all problem areas through a dedicated questionnaire circulated in December 2015 as well as dedicated meetings (meetings of the Financial Services Committee (FSC), on 17 February 2016).

In addition, all Member States FIUs were consulted in the context of the EU FIU platform (meeting of 26 January 2016). Following this meeting, Member States FIUs replied to a questionnaire dedicated to FIU related issues.

II. Targeted Stakeholder Consultation

a) The EDPS (European Data Protection Supervisor): the issues covered by the envisaged amendments of the directive were presented to the EDPS in a letter send 14 March 2016, in which the Commission asked for the EDPS' opinion, notably on all aspects relating to the data protection and privacy impact of the proposed measures.

b) With regard to other stakeholders, on virtual currencies and prepaid cards:

- Consumer organisations or equivalent via meetings (The European Consumer Organisation (BEUC), Finance Watch, Better Finance, Financial Service User Group (FSUG));
- Industry via meetings with Bitstamp, Circle, EMA (the Electronic Money Association), MasterCard, Visa, Raphaels Bank, Trust EU Affairs managing a

dedicated working group on virtual currencies gathering Oraclize, Bitwage, Scorechain, BitPay, Elliptic, Bitcoin Deutschland, Chain analysis and Coinify, experts from Edc@b, various financial institutions or representatives such as Intesa San Paolo or BAFT. Most industry representatives accepted to respond to the Commissions invitation under the condition that the views expressed would remain confidential;

- National authorities from outside the EU were also consulted such as the Japanese FSA and the US Treasury.

c) With regard to other stakeholders, on banking registries and enhanced customer due diligence (ECDD) measures:

- Physical meetings with financial sector representatives: European Banking Federation, European Banking Industry Committee representing the European Banking Federation, the European Association of Cooperative Banks, the European Savings Banks Group, the European Association of Public Banks, the European Federation of Buildings Societies, the European Mortgage Federation and Eurofinas-Leaseurop.
- Written consultation on ECDD measures and banking registries with the financial and insurance sector (European Banking Federation, Europe Insurance, European Association of Public Banks, Electronic money Association, MasterCard, Swift)[88]; with the gambling sector (European Casino Association and Remote Gambling Association); with legal professionals (Law Society).

The views by the different stakeholders, be it industry, consumers or national authorities, which were consulted are reflected under Sections 5 'Policy Options – Stakeholders views on the problem and options' and Section 6 about the analysis of the impact of the respective policy options proposed.

[88] We received contributions from British Bankers Association (BBA), Belgium Insurance Association, BGK Poland, Caixa General de Depositos, Belgian Financial Sector Federation, Deutsche Bank, Fédération Française des Sociétés d'Assurance, Finish Financial Services, Italian Banking Association, Lloyds Banking group, MoneyGram, PayPal, Western Union, ZH Insurance, Barclays, E-Money Association (EMA), MasterCard, Santander.

ANNEX 3: WHO IS AFFECTED BY THE INITIATIVE AND HOW?

Enhanced Customer Due Diligence requirements

In general, Member States and obliged entities see an interest in having more clarity about the ECDD measures to apply to high-risk third countries and in putting in place an harmonised and coordinated EU policy in that matter.

There will be no practical implications for the obliged entities that under their current practice already implement the list of ECDD measures provided by FATF recommendations (in relation to option A and B). This approach is recognised as beneficial, even for those who do not apply such a prescriptive list as it will give clearer guidance on how to manage business relationships with high-risk third countries and will enhance their capabilities to verify the data provided by a customer to detect suspicious activities. A prescriptive list, from a technical point of view, would facilitate an automated risk management processes and it may therefore limit the need for manual controls. In the consultation, the responding obliged entities were not in a position to provide a concrete costs implications of a harmonised approach on ECDD measures. Nevertheless, the cost benefit with automated processes will vary from one obliged entity to another. A coordinated approach also minimises the operational and reputational risks, which will result in financial benefits for the obliged entities.

Some Member States and obliged entities have expressed concerns about cost implications and the potential administrative burden caused by overly prescriptive rules (Option C) which they also considered to be opposed to the "risk based approach" principle. It cannot be excluded that that this option could affect de-risking in the financial sector even if the purpose with the EU listing is to include a mechanism that already exist at international level and on which financial institutions already rely.

All options will provide for a more consistent interpretation of ECDD obligations and will also ensure a level playing field at EU level.
As far as counter-measures are concerned (Option B), the list will be presented as illustrative only and will mainly bring legal certainty as regards the nature of such countermeasures and their differences with ECDD measures. In view of this it will not create new obligations or additional costs.

Virtual Currencies (VC)

VC exchange platforms and custodial wallet providers are affected by this initiative as they will have to put in place, if not already the case, customer due diligence and a mechanism of suspicious transactions report. The additional costs are described above. Max. cost of €5 000 000 for the whole EU industry (option C and E).

National authorities and a central authority will be affected having to put in place, at national level, a form for users to declare themselves. Central authority would be in charge of setting up the database and maintaining it. Costs described above and below 50.000 EUR for first year, less than €20 000 for maintenance. (Option B)

Finally, citizens will be affected (Option B) with no costs having to fill in a form on a national authority website to self-declare themselves as VC users.

Prepaid instruments

The prepaid card market segment at stake is a limited one and essentially concerns general purpose reloadable and non-reloadable prepaid cards. Travellers' cards as well as cards attributed through specific programmes such as corporate prepaid cards or prepaid cards used for the payment of social benefits or of immediate financial assistance are either subject to full CDD or an identification of the cardholder at the outset is already a common practice, if only because those entities attributing those cards need to know to whom and for what purpose, to avoid abuses by the beneficiaries.

Following discussions with market players, it appeared that the AML/CFT legislation through the setting of CDD exemption thresholds shaped the market for non-reloadable cards. In practice, no such cards can be found in the market with a value in excess of €250. More surprisingly, the core market for non-reloadable cards is represented by cards with values ranging from €25 to €150 (or up to £100).

The lowering of the current AML/CTF threshold, for instance from €250 to €125 or €150, would therefore leave prepaid card issuers unaffected, as market needs for non-reloadable cards could still be served without having to perform CDD and having consequently to support related costs. This would however mean that in inflationary times in future, this lower threshold could constrain the possible further development of that market segment. However, the current use by consumers of non-reloadable cards would remain unchanged, which is positive from a financial inclusion viewpoint.

The main impact concerns reloadable general purpose prepaid cards, which are the closest means of payment to a debit card linked to a payment account, which under today's AML/CFT requirements is subject to a full CDD.

A significant lowering of the threshold or its suppression means that for the market segment concerned, prepaid card issuers, which at least for the main ones, manage different programmes and types of prepaid cards, will need more time to recover their CDD costs.

Under the 3AMLD, a card could be reloaded up to €2 500 without having to be subject to a full CDD. Under the 4AMLD, stricter rules have been imposed with a monthly threshold of €250. CDD costs are estimated by industry at 2-3 to 5 euro. Taking the upper value, this means that for a 1% beneficiary margin, up to €500 have to be spent on a reloadable card before the €5 CDD cost can be absorbed. However, all depend on the defined programmes.

The actual occurrence of the cost under the 4AMLD will depend on the use of the card. In a programme in existence in one Member State, where the prepaid card is distributed by the post office, no reference in the information documentation is made to given amounts that would be determined by the AML legislation. It may therefore well be that depending on circumstances, a given cardholder might never trigger the thresholds defined either by the 3rd or the 4AMLD, whereas another cardholder might do so rapidly. Statistical information on the behaviour of cardholders is not publicly available and it is therefore not possible to assess actual costs.

The intensity of the impact on issuers will depend on the behaviour of their cardholders. In the worst-case scenario, issuers, compared to today's situation, will have to support a new CDD cost. Figures would amount to less than €10.6 million[89]. In the best-case scenario, the

[89] General purpose prepaid cards represent 2% of the 106 million prepaid cards issued in 2015, i.e. 2.12 million cards for a €5 CDD cost, or a €10.6 million total cost. This figure is inflated as the proportion of cards concerned encompasses both reloadable and non-reloadable cards. Under the proposed option, the AML/CFT regime for non-reloadable cards will entail

recovery of the costs that would in any case have been incurred under the current legislation will take longer than before as the timing of the CDD performance will be anticipated.

The impact on the profitability of prepaid card issuers will therefore be minimal and for the leaders, compounded by the diversity of their prepaid card programmes. Small 'monoliners' offering general purpose reloadable prepaid cards only might be more directly affected. However, the amounts at stake remain minimal.

Distributors would remain outside the scope of the 4AMLD and therefore would not be affected by the more stringent measures proposed.

Member States would not be affected in their supervisory efforts as prepaid card issuers are already 'obliged entities' under the EU AML/CFT legislation. FIUs might have potentially to address more suspicious transaction reports as a result of the more stringent AML/CFT requirements.

EU FIUs - enhanced powers and facilitated cooperation

The consulted stakeholders are generally strongly supportive for updating and aligning the 4AMLD with the latest international standards to clarify FIU powers (Option A). They would benefit from the amendment as this would both clarify that EU FIUs can obtain available information from any obliged entity in case of suspicion, even if this obliged entity did not previously report a Suspicious Transaction Report (STR), and that obliged entities should provide all necessary information directly to the FIU at its request. This option entails no additional obligations or cost for public stakeholders or businesses since it only clarifies the authority and competences of FIUs. The clarification would also have a positive effect in terms of enhanced cooperation between EU FIUs, for example the development of existing on-line IT-tools such as the FIU.net or help develop regulating "diagonal cooperation" between non-counterparts. There will be no practical implications for citizens/consumers.

The practical implications of the establishment of a single European FIU (Option B) are less clear for public administrations and this remains very sensitive since it implies both a substantial transfer of sovereignty and an extensive adaptation of national systems. This option would therefore benefit of further examination before the Commission can assess its full practical implications. Like Option A, it will have no practical implications for citizens/consumers.

Centralised registers or mechanisms allowing for a swift identification by FIUs of the identity of the holders of bank-and payment accounts

Member States will have costs for the creation of the IT-systems as well as yearly recurring costs for maintenance (Option A to C). On the basis of the selective sample of existing operational systems, the one-off cost are estimated to be between €170 000 and €1 200 000 and the recurring costs vary between €3 000 and €600 000. It is not possible to conclude that one option would create higher costs than the other in terms of establishment or maintenance. (Annex 7.4). The uploading of information into the IT-systems (by financial institutions or other actors) will generally be done through an automated IT-protocol.

---

no or hardly any additional CDD costs for issuers. The breakdown between both categories of cards is not available. The actual figures would be lower.

FIUs (and as the case may be, other AML/CFT competent authorities) will benefit in terms of swift access to relevant information on the accountholders that will not only speed up investigations but also make them more efficient and cost effective (see sample overview in Annex 7 point 3 of the high costs linked to the baseline scenario). Central databases or retrieval systems will also have a positive effect on cross-border cooperation and exchange of information as all national FIUs involved would have access to such information and well positioned to reply to requests from other EU FIUs.

According to the baseline scenario, the estimated costs for the financial sector/banks to examine and reply to blanket requests from FIUs are twice as high as the cost for the FIUs to request this information (Annex 7.3). The use of centralized mechanisms (Options A to C) will therefore also reduce the number of (irrelevant) request for information and the related costs for the financial sector. Finally, as explained in the assessment of the effectiveness of Options A to C, this targeted approach will also help financial institutions to better mitigate their reputational risks (linked to unknowingly performing banking services to criminals or terrorists), which will have a positive effect on the cost/benefit of their risk monitoring processes.

Holders of bank –and payment accounts: as regards data protection it should be noted that both options are limited to keeping only the necessary information into the centralized mechanisms and that the retention period for maintain the data available in the system after closing an account should be aligned with the already exiting retention period for personal data referred to in article 40 4AMLD.

ANNEX 4: ENHANCED CUSTOMER DUE DILIGENCE

1/ Current framework related to business relationships involving high-risk third countries

- **Directive (EU) 2015/849 – 4AMLD**

Third-country policy

Article 9

1. Third-country jurisdictions which have strategic deficiencies in their national AML/CFT regimes that pose significant threats to the financial system of the Union ('high-risk third countries') shall be identified in order to protect the proper functioning of the internal market.

2. The Commission shall be empowered to adopt delegated acts in accordance with Article 64 in order to identify high-risk third countries, taking into account strategic deficiencies, in particular in relation to:

(a) the legal and institutional AML/CFT framework of the third country, in particular:

(i) criminalisation of money laundering and terrorist financing;

(ii) measures relating to customer due diligence;

(iii)requirements relating to record-keeping; and

(iv)requirements to report suspicious transactions;

(b) the powers and procedures of the third country's competent authorities for the purposes of combating money laundering and terrorist financing;

(c) the effectiveness of the AML/CFT system in addressing money laundering or terrorist financing risks of the third country.

3. The delegated acts referred to in paragraph 2 shall be adopted within one month after the identification of the strategic deficiencies referred to in that paragraph.

4. The Commission shall take into account, as appropriate, when drawing up the delegated acts referred to in paragraph 2, relevant evaluations, assessments or reports drawn up by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, in relation to the risks posed by individual third countries.

***

Enhanced customer due diligence

Article 18

1. In the cases referred to in Articles 19 to 24, and when dealing with natural persons or legal entities established in the third countries identified by the Commission as high-risk third

countries, as well as in other cases of higher risk that are identified by Member States or obliged entities, Member States shall require obliged entities to apply enhanced customer due diligence measures to manage and mitigate those risks appropriately.

(…)

3. When assessing the risks of money laundering and terrorist financing, Member States and obliged entities shall take into account at least the factors of potentially higher-risk situations set out in Annex III.

***

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(…)

(3) Geographical risk factors:

a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

- **The Financial Action Task Force recommendations (February 2012)**

Interpretative note Recommendation 10

"Higher risks

15. There are circumstances where the risk of money laundering or terrorist financing is higher, and enhanced CDD measures have to be taken. When assessing the money laundering and terrorist financing risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher-risk situations (in addition to those set out in Recommendations 12 to 16) include the following:

(…)

(b) Country or geographic risk factors:

a. Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems.
b. Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations.
c. Countries identified by credible sources as having significant levels of corruption or other criminal activity.
d. Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(…)

Enhanced CDD measures

20. Financial institutions should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, financial institutions should be required to conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

a) Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
b) Obtaining additional information on the intended nature of the business relationship.
c) Obtaining information on the source of funds or source of wealth of the customer.
d) Obtaining information on the reasons for intended or performed transactions.
e) Obtaining the approval of senior management to commence or continue the business relationship.
f) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
g) Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards."

***

Recommendation 19

"19. Higher-risk countries

Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF.

Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks".

***

Interpretative note recommendation 19

"1. The enhanced due diligence measures that could be undertaken by financial institutions include those measures set out in paragraph 20 of the Interpretive Note to Recommendation 10, and any other measures that have a similar effect in mitigating risks.

2. Examples of the countermeasures that could be undertaken by countries include the following, and any other measures that have a similar effect in mitigating risks:

a) requiring financial institutions to apply specific elements of enhanced due diligence.

b) introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions.

c) refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;

d) prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems;

e) limiting business relationships or financial transactions with the identified country or persons in that country;

f) prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process;

g) requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned;

h) requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned;

i) requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned"

2/ FATF listing of countries having deficient AML/CFT regimes (last publication 19 February 2016)

Listing process	Jurisdictions concerned	Consequences
FATF black list *"public statement*": countries with strategic deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with FATF to address them.	**2 jurisdictions** **Iran; Democratic People's Republic of Korea (DPRK)** = call for countermeasures	Rec 19: countries should be able to apply **countermeasures when called upon to do so by the FATF**
FATF grey list *"improving global AML/CFT compliance countries*: ongoing process": countries selected from the ICRG pool or designated by FATF members that are involved in an action plan with FATF to address their deficiencies.	**11 jurisdictions** **Afghanistan, Bosnia and Herzegovina, Guyana Iraq, Lao PDR, Myanmar, Papua New Guinea, Syria, Uganda, Vanuatu, Yemen**	NR10: There are circumstances where the risk of ML/TF is higher and **enhanced CDD measures** have to be taken: countries identified by credible sources such as mutual evaluation or detailed assessment reports or published follow-up reports as not having adequate AML/CFT systems.

3/ Summary of the written consultation – private sector

- **Business exposure, application of customer due diligence and impacts**

	What is your business exposure to high-risk third countries (extent and, where possible, volume)	**Do you apply different level of CDDs according to the "category" of FATF lists (i.e. Public Statement list/Improving compliance list)?**	**How do you assess the impacts of harmonised ECDD measures (+), (-) or (0)**
Obliged entity 1	Limited	Individual assessment of each case involving countries listed by FATF and own list	impacts (-) cost and over prescription if one fits all approach impacts (+) authoritative guide for companies who rarely deal with non-domestic business and level playing field
Obliged entity 2	No business with Iran, Cuba, Sudan, North Korea, Syria Limited business with other countries	/	impact (0) as most of these measures are already applied impact (+) more transparency and easiest disclosure of information at EU level on initiator and beneficiary of payments
Obliged entity 3	Limited (289 customers) and passive business relationship. Negligible business volume	No distinction - Each country of any of the FATF lists is considered as high risk and subject to EDD	impact (+) clarification of the processes
Obliged entity 4	/	/	impacts (-) costs because of additional IT impacts (+) processes will be automated and will ease the investigative functions; level playing field avoiding gaps in national legislations
Obliged entity 5	Business worldwide except Iran and North Korea but through licensed EEA institutions. Countries most concerned: Afghanistan, Algeria, Angola, Bosnia, Iraq, Guyana, Panama, Papua New Guinea, Syria, Uganda, Yemen and Laos	No distinction - Each country of any of the FATF list is considered as high risk	impact (0) as no direct relationships with high-risk third countries impact (+) less complexity and more simple oversight by regulators impact (-) if too prescriptive rules
Obliged entity 6	Limited exposure	No distinction - Each country of any of the FATF list is considered as high risk	impacts (-) costs and technical developments for SMEs impact (+) harmonised approach would bring more clarity on the legal requirements and enhance cooperation

Obliged entity 7	Limited (1-4 transactions per year)	No distinction - Each country of any of the FATF list is considered as high risk	impact (+) reputational and operational risks are minimized impact (-) technical costs
Obliged entity 8	Very low, less than 1%	Yes - Public statement countries are monitored more closely	impact (+) consistency across the business sector will reduce the risks impact (-) if too prescriptive rules
Obliged entity 9	Only 1,56% of customers base	Yes - Risk based approach and risk monitoring is different depending on the country concerned	impact (-) highly prescriptive rules would contradict the risk based approach
Obliged entity 10	/	Yes - Public statement countries are monitored more closely	impact (+) consistent interpretation and application will improve the ability to limit the risks impact (-) technical implementation and timeline for IT upgrades
Obliged entity 11	/	Yes - Risk based approach and risk monitoring is different depending on the country concerned	impact (+) less complexity and more simple oversight by regulators impact (-) highly prescriptive rules would contradict the risk based approach
Obliged entity 12	Volume of activities not specified information on the volume	No distinction - Each country of any of the FATF lists is considered as high risk and subject to EDD	impact (+) more certainty for obliged entities on AML/CFT requirements but additional ECDD measures will contradict the RBA application
Obliged entity 13	very limited	No distinction - Each country of any of the FATF lists is considered as high risk and subject to EDD	impact (+) harmonisation at group level of EDD measures and level playing field avoiding gaps in national legislations impact (-) costs
Obliged entity 14	very low	Yes - Risk based approach and risk monitoring is different depending on the country concerned	impact (+) enhance obliged entities' capabilities to verify the data and to detect anomalies and suspicious activities impact (-) too prescriptive rules may bring costs and would contradict the risk based approach

Obliged entity 15	/	/	impact (+) level playing field avoiding gaps in national legislations impact (-) if systematic approval of senior management or systematic reporting of the transaction
Obliged entity 16	no business relationships with high-risk third countries	No distinction - Each country of any of the FATF lists is considered as high risk and subject to EDD + own list	impact (+) clarification of the requirements especially for actors operating in several jurisdictions
Obliged entity 17	no business relationships with high-risk third countries	/	impact (+) no room for interpretation, less risk of regulatory sanctions impact (-) if too complex rules
Obliged entity 18	very limited	No distinction - Each country of any of the FATF lists is considered as high risk and subject to EDD	impact (+) level playing field avoiding gaps in national legislations
Obliged entity 19	less than 2% of clients	/	/
Obliged entity 20	very low no presence in Iran, North Korea, Afghanistan, Iraq, Myanmar, Syria send only in Guyana, Laos, Papua New Guinea, Uganda, Vanuatu, Yemen send/receive/withdraw Bosnia Herzegovina	Yes - no services offered in countries listed in the Public Statement; limited services offered in other countries listed	impact (0) as the risk management program for high-risk third countries is already really robust and in line with the harmonization plan proposed impact (+) level playing field avoiding gaps in national legislations
Obliged entity 21	no business relationships with high-risk third countries	Yes - Public statement countries are monitored more closely	impact (0) limited business exposure

- **<u>Current implementation of Enhanced customer due diligence measures (</u>based on FATF recommendations)**

How do you concretely apply the following enhanced customer due diligence measures to high-risk third countries?							
	1/ additional info on the customer	**2/ additional info on the intended nature of business relationship**	**3/ information on the source of funds**	**4/ information on the reasons for intended or performed transaction**	**5/approval of senior management**	**6/ enhanced monitoring**	**7/ first payment carried out through an account**
Obliged entity 1	open source information and self-declaration with documentary verification	open source information and self-declaration with documentary verification	evidence of the customer's funding account (bank statement)	customer information and assessment as to whether the activity is what is expected to see	escalation process up to Board level for highest risk business. MLRO drive any recommendations to refuse business	possible to "block" accounts where risk warrants formal AML team and MLRO approval	no fulfilment of this requirement triggers additional CDD
Obliged entity 2	checks in external database, adverse negative press check	transaction volumes and transactions flows (financial institutions); trade finance services (corporate clients)	source of capital and check of wealth of the UBO (legal entity); source of wealth (natural person)	questions on the reason for opening a non-resident account	yes but no specific elements mentioned	yes but no specific elements mentioned	yes but no specific elements mentioned
Obliged entity 3	request to the client via his relationship manager and via external sources	request to the client via his relationship manager and via external sources	request to the client via his relationship manager and via external sources	request to the client via his relationship manager and via external sources	within compliance department	automatic detection of new relationship and automatic detection of all linked transactions (above a certain amount)	no
Obliged entity 4	extended questionnaire	extended questionnaire	specific questionnaire source of wealth for high value individuals, free format for others	extended questionnaire	for highest risk only (decision to commence or continue a business relationship)	yes for adapted and specific scenarios	manual check (only in some cases)
Obliged entity 5	documentary evidence, employment, source of funds.	EDD at the time of the transaction where appropriate	EDD at the time of the transaction where appropriate	EDD at the time of the transaction where appropriate	for highest risk only (e.g. Politically exposed persons)	sophisticated real time automated monitoring system	in limited circumstances
Obliged entity 6	specific templates to request additional information on customers	yes but no specific elements mentioned	yes but no specific elements mentioned	yes but no specific elements mentioned	only for Politically exposed persons	yes but no specific elements mentioned	not always

Obliged entity 7	yes (100% cases) but no specific elements mentioned	yes (100% cases) but no specific elements mentioned	non relevant for the activity concerned	non relevant for the activity concerned	yes (100% cases) but no specific elements mentioned	yes (100% cases) but no specific elements mentioned	yes (100% cases) due to the activity concerned (still bank intervening)
Obliged entity 8	yes (100% cases) but no specific elements mentioned	/	yes (100% cases) but no specific elements mentioned	/	/	yes (100% cases) but no specific elements mentioned	yes (100% cases) but no specific elements mentioned
Obliged entity 9	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned	for all cases of concern and the decision process.	/	/
Obliged entity 10	yes (most frequent) but no specific elements mentioned	yes (moderate) but no specific elements mentioned	yes (moderate) but no specific elements mentioned	yes (moderate) but no specific elements mentioned	yes (moderate) but no specific elements mentioned	yes (moderate), e.g. limitation the transaction amounts or volumes of transactions, enhanced monitoring controls, stopping the customer from transacting until EDD are completed	yes-most frequent (and maybe recurring when customer is using a credit or debit card)
Obliged entity 11	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)
Obliged entity 12	additional documents, data or information to establish the identity; supplementary measures to verify or certify the documents; electronic verification;	supplementary measures to verify or certify the documents	supplementary measures to verify or certify the documents	supplementary measures to verify or certify the documents	supplementary measures to verify or certify the documents	supplementary measures to verify or certify the documents	yes but no specific elements mentioned
Obliged entity 13	yes but no specific elements mentioned	yes but no specific elements mentioned	no	yes but no specific elements mentioned	yes but no specific elements mentioned	yes but no specific elements mentioned	no

Obliged entity 14	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)	yes but on a risk sensitive basis (manual checks of additional information and supporting documents)
Obliged entity 15	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned	non relevant for the activity concerned
Obliged entity 16	systematic (not only for high risk customers)	for high risk customers	check whether transaction fits into client's regular transaction pattern	yes for PEPs relationships	yes but no specific elements mentioned	systematic	systematic
Obliged entity 17	Commercial databases, collection of statement of the clients	Commercial databases, collection of statement of the clients	Commercial databases, collection of statement of the clients	Commercial databases, collection of statement of the clients	Commercial databases, collection of statement of the clients	moderate use but no specific elements mentioned	moderate use but no specific elements mentioned
Obliged entity 18	systematically to all countries listed by FATF	systematically to all countries listed by FATF	systematically to all countries listed by FATF	systematically to all countries listed by FATF	systematically to all countries listed by FATF	systematically to all countries listed by FATF	systematically to all countries listed by FATF
Obliged entity 19	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases	systematic when customer is not physically present, is a PEP or for correspondent banking + risk sensitive basis for the other cases
Obliged entity 20	systematic manual review for high risk customer behaviours	systematic manual review for high risk customer behaviours	systematic manual review for high risk customer behaviours	systematic manual review for high risk customer behaviours	systematic manual review for high risk customer behaviours	systematic manual review for high risk customer behaviours	/
Obliged entity 21	yes (+50% cases) but no specific elements mentioned	no	yes (+25% cases) but no specific elements mentioned	yes but no specific elements mentioned	yes (+25% cases) but no specific elements mentioned	yes but no specific elements mentioned	yes but no specific elements mentioned

ANNEX 5: VIRTUAL CURRENCIES AND PREPAID INSTRUMNENTS

a) The Virtual Currency market

i) Main market players / Definitions

Various stakeholders are involved in the virtual currency market with the main ones being:

- **User[90]:** a person or legal entity that obtains Virtual Currencies (VC) and uses it to purchase real or virtual goods or services, or to send remittances in a personal capacity to another person (for personal use), or who hold the VC for other purposes, such as an investment. Typically users can obtain VC in one of the following three ways:
    - through an exchange (or, for most centralised VCs, directly from the entity governing the scheme) using Fiat Currencies (FC) or some other VC;
    - engaging in specific activities, such as responding to a promotion, completing an online survey, 'mining' (running special software to solve complex algorithms to validate transactions in the VC system); and/or
    - receiving VC from the scheme governing entity, the issuer or another user who is acting for purposes other than his or her trade, business or profession.

  With an objective of simplification, we include merchants accepting VCs under this category.

- **Miners:** in decentralised VC schemes, miners solve deliberately complex algorithms to obtain small amounts of VC units. Miners tend to operate anonymously, from anywhere in the world, and validate VC transactions. When a group of miners controls more than half the total computational power used to create VC units, the group is potentially in a position to interfere with transactions, for example by rejecting transactions validated by other miners. Miners group into pools of miners (Antpool, F2Pool, BitFury, BTCC Pool, BW.COM…). Currently, most miners are located in China.

- **Wallet providers:** users may hold their VC accounts on their own devices or entrust a wallet provider to hold and administrate the VC account (an e-wallet) and to provide an overview of the user's transactions (via a web or phone-based service).

  We will distinguish two types of wallets providers:
    - software wallets providers and
    - custodial wallets providers (including multi-signature wallets).

  Contrary to software wallet providers that provide applications or programs running on users hardware (computer, smartphone, tablet…) to access public information from a distributed ledger and access the network, custodial wallet providers include the

[90] All definitions extracted from the EBA Opinion on virtual currencies

custody of the user's public and private key. **Compared to traditional financial services, they are quite close to bank accounts.**

Wallets can be stored both online ('hot storage') and offline ('cold storage'), the latter of which increases the safety of the balance by protecting the wallet.

- **Exchange platforms:** a person or entity engaged in the exchange of VC for FC, FC for VC, funds or other brands of VC. Exchanges may generally accept a wide range of payments, including cash, credit transfers, credit cards and other VCs. Comparable to traditional currency exchanges, the larger VC exchanges provide an overall picture of the changes in a VC's exchange price and its volatility. Some exchanges may offer services to their clients, such as conversion services for merchants who accept VCs as payment, but fear a depreciation risk and would immediately like to convert any incoming VC-payments into a (national) fiat money of their choice.

  Compared to traditional financial services, they are the "bureau de change" of the virtual currency world.

  ATMs are included under this category.

ii) The VC market

Official data regarding the market is hard to reach. However, based on various websites[91] tracking volumes and prices of exchanges or conducting research, the following estimations could be given. These were checked during interviews conducted with market players – who tended to provide lower estimates than the statistics found online. Hence, the following statistics should reflect a upper-level but balanced estimation:

Total VC wallets worldwide	13 million (Q4 2015)[92] – 7.4 million in Q4 2014
VC wallets in the EU	About 3 million
VC users worldwide[93]	From 1 to 4 million
VC users in the EU	About 500.000
VC miners worldwide	100.000[94]
VC miners in the EU	10.000 (estimate)
VC software wallet providers worldwide	> 500 (estimate)
VC custodians worldwide	> 100(estimate)
VC custodians in the EU	> 20 (estimate)
Exchange platforms worldwide	> 100
Exchange platforms in the EU	> 28
ATMs worldwide[95]	571
ATMs in the EU	> 100
Daily VC transactions	> 125.000 (bitcoin only - for 2015)
Merchants accepting bitcoins	110.000 (Q4 2015) – 80.000 in Q4 2014
Market capitalisation of VCs	€7 billion

[91] See for instance http://exchangewar.info/, http://coinmarketcap.com/exchanges/volume/24-hour/ or websites indicated below

[92] http://www.coindesk.com/state-of-bitcoin-blockchain-2016/ Slide 8

[93] At least one transaction per month

[94] http://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/

[95] http://coinatmradar.com/ (consulted 4.2.2016)

The uptake of VCs can be explained by various factors which include:

- **Speculative investment opportunities** (based on discussions with major exchange platforms and custodians, 90 to 95% of transactions are linked to speculation / investment / trading)

- Benefits of VCs when used as payment methods (about 5 to 10% of the volumes) compared to other products available for international transfers, such as money remittances:
    - **Speed:** a transaction confirmation takes approximately 10 minutes. Some merchants are willing to provide products or service before the transmission has been confirmed by a miner and added to the blockchain. This action also known as a Zero-confirmation transaction carries a risk of double spending.
    - **Low cost:** transactions can be processed for free
    - **Micro payments:** VCs can be fragmented to very low amounts. For instance bitcoins can be fragmented to btc 10^{-8} (also called a satoshi) – which in combination with their low cost of processing, could represent significant new opportunities in the market for payment for micro transactions
    - **Financial inclusion** (replacing bank accounts by VC wallets, allowing international transfers at a lower cost than traditional money remitters). As indicated in the IMF paper, the global average cost of sending small remittances is 7.7% when it is estimated to be 1% with bitcoin.
    - **Security, trust and transparency** through the use of distributed ledgers
    - **Anonymity:** as defined in a recent International Monetary Fund staff discussion note[96], *most cryptocurrencies are "pseudo-anonymous": while cryptocurrency transactions are publicly recorded, users are known only by their VC "addresses," which cannot be traced back to users' real-world identity. As such, cryptocurrency transactions are more transparent than cash but more anonymous than other forms of online payment.*

- Finally, **the philosophy behind VC** is attractive as it is based on democracy and consensus

It could however be argued that most of the benefits do not materialise in practice. For instance, transactions are not completely free as fees can be added to the transaction by users and miners receive newly mined currencies for validating transactions, a reward that disappears once the total number of units of a currency is reached. Compared to SEPA products, for instance, and even more considering the future release of instant payments in euro, VCs cannot compete. Many Virtual Currencies have already disappeared (more than 400) and the "deadpool" of virtual currencies company is already quite large (26 start-ups at Q4 2015[97]).

[96] https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

[97] http://www.coindesk.com/state-of-bitcoin-blockchain-2016/ Slide 17

The low cost benefit aspect remains true for international payment / money remittances. However, exchange fees from VC to FC and back can go up to 10% through ATMs.

Finally, VCs may increase financial inclusion but the use of VCs still requires minimum IT equipment (at least a smartphone and internet connection).

iii) Current legislation

Virtual currencies are currently not regulated at EU level but some Member States have taken action or are considering action as reported by them below:

- Germany: BaFin qualified Bitcoins as "Rechnungseinheiten" (units of account under German law) in August 2011 and, therefore, as financial instruments in accordance with section 1 (11) of the Banking Act (Kreditwesengesetz – KWG). If Bitcoins are traded as such, contrary to their actual function, they are deemed to be financial instruments requiring authorisation in accordance with section 1 (1a) sentence 2 nos. 1 to 4 of the KWG. In accordance with section 1 (1a) of the KWG, the trading must be conducted commercially or on a scale which requires a commercially organised business undertaking. Key examples of this are proprietary trading (the purchase and sale of financial instruments for one's own account as a service for others), and investment broking (broking transactions, including via Internet platforms, to purchase and sell financial instruments). If such transactions are carried out for a commission, they may also be considered to be principal broking services under section 1 (1) sentence 2 no. 4 of the KWG and, as such, banking business requiring authorisation. In addition, this means that in such cases trading-business falls under the scope of the German Anti-Money Laundering Act. Obliged persons and entities have inter alia to identify and verify their customers and to have ongoing monitoring measures in place.

- Estonia: As determined in Art. 6(4) of the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) a provider of services of alternative means of payment is a person who in its economic or professional activities and through a communication, transfer or clearing system buys, sells or mediates funds of monetary value by which financial obligations can be performed or which can be exchanged for an official currency, but who is not a person specified in subsection (1) or a financial institution for the purposes of the Credit Institutions Act (CrIA). Providers of services of alternative means of payment are required to be registered in the register of economic activities before commencing operations (Art. 52 of the MLTFPA). The definition of "provider of services of alternative means of payment" has been set out in the MLTFPA to cover means of payment which are increasingly being performed in different electronic channels, which cannot be considered traditional methods of payment. New unconventional electronic payment systems are not usually account-based. A similar element of alternative systems is that they allow a party to a

transaction to transfer money/value immediately, conveniently, securely and anonymously. The providers of alternative means of payment have been obligated persons since 2008. According to MLTFPA they have to apply all due diligence measures and other measures as financial institutions and other special requirements set out in Art. 15(8).

- France: On 29 January 2014, the French Prudential Supervisory and Resolution Authority (ACPR) issued a position statement, emphasizing that an entity engaged in intermediation with respect to the purchase or sale of VC in exchange for fiat currency is a financial intermediary which receives funds on a third party's behalf, and that these activities shall only be performed by payment service providers duly authorized to carry out activity in France (credit institution, payment institution or electronic money institution). Such operations are subject to relevant AML/CTF regulations under the control of the ACPR. However, it is important to note that this Position is not applicable to all virtual currency exchange platforms. Indeed, platforms which buy virtual currencies for their own account in order to sell them to buyers are not subject to this Position. Only platforms providing a service of fund transfer between buyers and sellers are concerned.

- Luxemburg: The CSSF informed that it considers “virtual” currencies as money, since they are accepted as a means of payment of goods and services by a sufficiently large group of people. More specifically, it clarified that virtual currency constitutes scriptural money as opposed to cash in the form of banknotes and coins. The scriptural nature does not require a tangible writing, similarly to electronic documents or signatures that do not require paper. Virtual currencies may thus be electronic money, but not necessarily within the meaning of the European Directive 2009/110 which provides for a definition of electronic money limited to its own scope. The CSSF also drew the attention to the fact that the issuing of virtual currencies is not regulated from a monetary point of view and that the methods for its issuing and the definition of its relation with other monies may vary from one type of virtual currency to another. Virtual currencies are obviously not legal tender and they entail risks for their holders. The CSSF also referred to the public warning issued by the EBA and ESMA on the subject of the different risks associated with virtual currencies.

- Sweden: The FSA has deemed that virtual currency exchange platforms provide means of payments. By law, such activities require a registration as financial institutions.

- The UK is exploring how to bring digital currency exchanges carrying out the activities of digital-fiat exchange into the scope of the AML/CTF regulation, including the potential expansion of the fourth anti-money laundering Directive (4AMLD). The detail of this regulatory regime will be discussed in a forthcoming consultation, to be published early in 2016.

- The Court of Justice of the European Union ruled in a decision of 22 October 2015[98] that the exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT.

The FATF, EBA, ECB and Bank for International Settlements have all issued studies and, FATF and EBA also issued recommendations concluding that virtual currencies exchange platforms are at least brought within the scope of the AML/TF framework. Although, on the basis of this evidence, the Commission proposed to include VC platforms into the 4AMLD at a relatively late stage of the negotiations, it proved too late in the process to secure sufficient support of Member States and the European Parliament.

EBA even suggests, in addition, a long term approach to provide a full regulatory framework for virtual currencies.

Since this time, the level of consensus about the need for action in this area has considerably risen. Nearly all EU Member States have issued warnings to consumers (24 out of 28 Member States) and MS that were opposed to legislation in 2014 are now open to it or even proposed national legislation.

Outside the EU, it is to be noted that the New York State Department of Financial Services issued in 2015 a regulation related to the conduct of business involving VC (BitLicense)[99], which includes capital requirements, consumer protection, reporting and AML requirements (internal controls, policies, procedures to comply with AML Regulation, independent testing of the program in place, compliance officers, training, CDD, transaction reporting, suspicious activities reporting…) and cybersecurity rules that will be applied to exchange platforms and custodial wallet providers.

[98] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf

[99] http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

Market players	Population	Risk addressed	Current status	Approximation "regulated" world	Policy options	+ Arguments	- Arguments	Option rating
Users	1 to 4 million worldwide 500k in the EU 110k merchants worldwide	ML/TF use of VCs facilitated by anonymity	Unregulated	Consumers, merchants	Remain unregulated	• Anonymity can be lifted through targeting other market players (exchange platforms and/or custodian wallet providers)	• Anonymity remains for users not going through regulated portals	+
					Prohibit the use of VCs	• Addresses the risk	• Drastic solution (far beyond target) • May stifle innovation • Not enforceable (number of users, global phenomenon)	--
					Mandatory registration of users	• Anonymity lifted	• Hardly enforceable (number of users, global phenomenon)	-
					Self-declaration of users on a voluntary basis	• **Anonymity partially lifted by voluntary users**	• **No obligation for users.**	+
Miners	100k worldwide 10k in the EU	ML/TF use of VCs facilitated by anonymity (capacity to obtain VCs without exchange)		Infrastructure (Scheme / Clearing / Settlement through the DL/Blockchain)	**Remain unregulated**	• **Anonymity can be lifted through targeting other market players (exchange platforms and/or wallet providers)**	• **Criminals investing in mining and receiving VCs do not go through any KYC as long as they remain in the VC ecosystem**	++
					Registration / Supervision of miners	• Address the risk of criminal miners	• May stifle innovation • Not enforceable (number of miners, global phenomenon)	-
Exchange platforms (ATMs included)	At least 103[1] online exchange platforms globally At least 28 online exchange platforms have EUR / VC capabilities 571 ATMs worldwide 100 ATMs in the EU	ML/TF when exchanging/converting VCs (for FC and vice versa)		Exchange office / Bureau de change	Remain unregulated	• Anonymity can be lifted through targeting other market players (wallet providers) • No burden on exchange platforms	• No AML/CFT regime. No supervision of the market • Easier ML/FT activities. VCs become "place to invest" for criminals • National measures put in place – Regulatory arbitrage	-
					Bring them under 4th AMLD for CDD requirements	• **Limited population** • **AML/CFT requirements applied for all exchanges** • **Easily done through AMLD4** • **Supervision and suspicion reports**	• **Does not capture all exchanges (local p2p exchanges out as well as all VCs that are not cashed out)** • **Global scale enforcement**	++
					Bring them under PSD2 for licensing	• Automatically covered by ALMD4 • Additional measures for consumer protection	• Does not capture all exchanges (local p2p exchanges out as well as all VCs that are not cashed out) • Longer time to market vs AMLD4 • Global scale enforcement	+
					Prohibit exchange platforms	• Addresses the risk	• Drastic solution (far beyond target) • Not enforceable given the global scale	--
Wallet providers (custodian)	+/- similar to exchange platforms (estimate)	ML/TF risk when spending VCs		Banks	Remain unregulated	• Anonymity can be lifted through targeting other market players (exchange platforms) • No burden on wallet providers	• No AML/CFT regime. No supervision of the market • Easier ML/FT activities. VCs become "place to invest" for criminals • National measures put in place – Regulatory arbitrage	-
					Bring them under 4th AMLD for CDD requirements	• **Limited population** • **Lift of anonymity on VC transactions within the VC world** • **Captures a wide range of transfers**	• **Global scale enforcement**	++
					Bring them under PSD2 for licensing	• Automatically covered by ALMD4 • Additional measures for consumer protection / safeguarding of funds	• Global scale enforcement • Longer time to market vs AMLD4	+
					Prohibit wallet providers	• Addresses the risk	• Drastic solution (far beyond target) • Not enforceable given the global scale	--

b) The Prepaid instruments market

The analysis of the EU prepaid card market is the result of interviews conducted between early December 2015 and February 2016 with representatives of the prepaid card industry (3 meetings), two global card schemes (4 meetings) and two major prepaid instrument issuers (2 meetings), and statistical data provided by the profession and the ECB.

i) Market volume

Available statistics on the prepaid card market are few and the main sources used, which both have their shortcomings as a result of their partial coverage, are the public statistics of the European Central Bank (ECB) which do not cover all Member States for this purpose and those compiled by the European e-Money Association (EMA) on the basis of data provided by its members. The quality of data is globally poor and those data are very difficult to recoup, as available data sets do not necessarily cover the same universes.

The ECB gathers data on the e-money market which represents a larger universe covering both prepaid instruments (prepaid cards –whether virtual or plastic ones- or vouchers) and account-based e-money (e.g. PayPal).

According to the ECB data on the e-money market, in 2014, e-money payment transactions for the 22 Member States[100] that provided data amounted to €73 billion corresponding to e-money payment transactions with e-money issued by EU resident payment service providers. This amount of €73 billion includes 57 billion in LUX (Pay-Pal, Amazon) and 13 billion in IT. The number of transactions was 2.09 billion (including 1.5 billion in LUX and some 300 million in IT). These data are not complete as they do not include several non-euro area markets notably UK, SE, DK and PL and therefore underestimate the actual size of the EU market. The average transaction value on that basis was of €35. E-money payments represented 3% of the total number of electronic payment transactions in the euro area (EU-18). In the last 5 years (2010-2014), the number of e-money transactions in the EU increased 2 times, and their value 2.5 times.

On the basis of the ECB statistics, the prepaid instrument market in 2014 would have represented €19.3 billion[101], out of which 13 billion are attributable to the IT prepaid cards which are essentially distributed by a public body, Poste Italiane, and 3.2 billion to the UK market, which is the second in size in the EU. The ECB statistics do not cover limited network markets, including the gift card market. However, these cards are outside the scope of the AML/CTF legislation, at EU or national level, as their use is restricted to limited networks of retailers, or petrol stations (for fuel cards), and hence such cards present low AML/CTF risks.

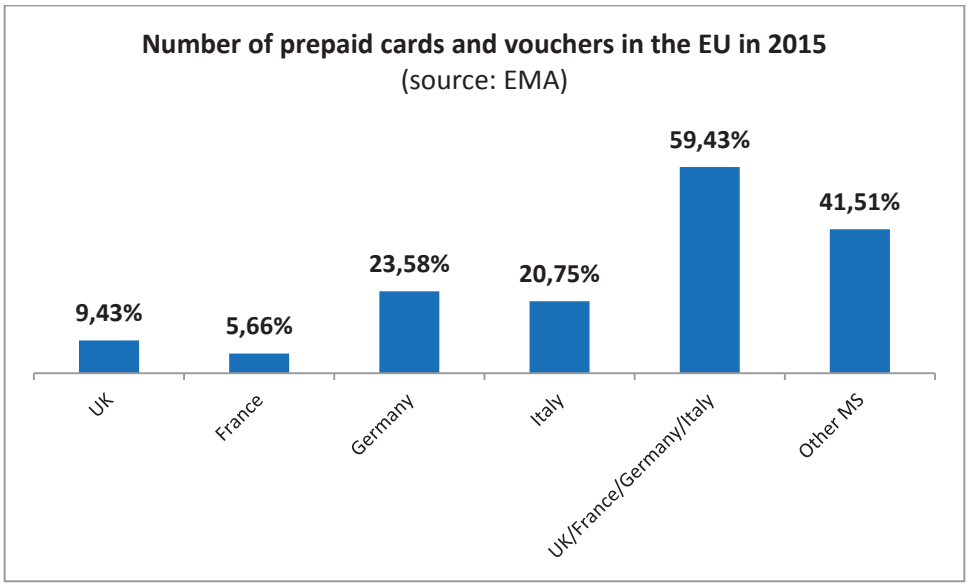
A major international card scheme is of the view that the global prepaid card market in Europe (in the broad sense, Russia, Ukraine and Turkey being included in its data) will reach 149 billion USD in value in 2017. Such figures are market estimates and include closed-loop cards such as gift cards.

[100] No data reported for DK, EE, LT, PL, SE and UK.

[101] Estimate obtained by subtracting from the global figure provided by the ECB (€73 billion), the amount attributed to the e-money activities of PayPal and Amazon which are essentially account-based e-money ones, and adding the data available for the UK (source EMA), i.e. €3.3 billion.

According to the European e-Money Association (EMA), the total of cards and vouchers issued in 2015 in the EEA was approximately of 106.000.000, a number which of course is lower than the total number of cards and vouchers in circulation.

Four Member States only (the UK, Italy, Germany, France) make 59% of the EEA prepaid card market.



The peculiarity of the Italian prepaid card market is largely due to the fact that the domestic debit card, PagoBancomat, can neither be used online nor abroad, that there is diffidence about using one's credit card to buy online due to the risk of payment fraud, and also to the fact that bank accounts are considered expensive. Hence, the popularity of prepaid cards which are used to buy goods and services online, to travel and as a substitute to bank accounts.

ii) Description of the EU market

In Europe, the prepaid instrument market essentially is a prepaid card market. Only one sizeable operator still offers prepaid paper vouchers distributed through retailers. However, these paper products are progressively abandoned for plastic cards, which particularly if equipped with a chip, offer more versatility and uses for the consumer.

Prepaid cards have started developing at the end of the 1990s as an alternative to debit cards (which require the existence of a payment account at a bank or a financial institution) and to credit cards (which require the card issuer to evaluate the cardholder's minimum level of creditworthiness). Prepaid cards began as a device used to pay for goods and services where the issuer does not need to conduct any analysis on the cardholder's credit standing, or the cardholder bear the costs for opening and maintaining a payment account.

The prepaid card market is a complex one, basically a sum of niche products, presenting different characteristics in different jurisdictions in terms of weight, products or distribution channels. Prepaid cards can be offered as one-off solutions (typically in limited networks as technology based on magnetic stripe, not electronic chip) or reloadable cards. Besides the cards, there are other solutions in the market taking the form of paper vouchers or even mobile phone credits, when the latter can be used to buy other services than telecom ones. Whilst these instruments are little used compared to cards, any

action regarding prepaid cards should more generally apply to prepaid instruments to avoid substitutive effects.

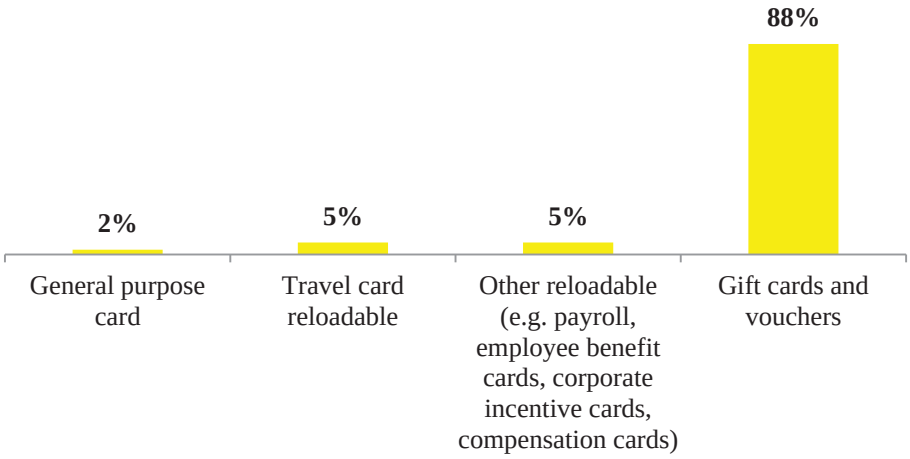
Two well-known global card schemes are the major providers of prepaid cards in Europe. A third international card scheme has a very small share of the market and there is limited competition from some domestic card schemes and from some card processors.

The different types of prepaid cards

Many prepaid cards are used in **limited networks**, for instance gift cards, prepaid fuel cards for use at a given brand of petrol station, or cards whose use would be limited to a chain of retail stores (*closed loop prepaid cards*), or to a given shopping centre (*semi-open loop prepaid cards*), or to buy lunch. Gift cards[102] are an important market segment for prepaid cards (representing €6 billion in the UK only). Gift cards can generally be used domestically only, cannot be used to withdraw cash at ATMs and are sometimes not allowed for online use. All these parameters are defined by the e-money issuer. The acceptance of a foreign gift card by a merchant would require that the latter be equipped with an online terminal capable of reading the card (like for a pre-authorised debit card), which would be too complex and costly for the acquirer. International card schemes are present on this market. By construction, gift cards are not nominative, as they are to be attributed by their buyers to the beneficiaries of the gift, for instance by a grand-mother to her grand-daughter. The issuer of the gift card does not know who will buy a given gift card for whom, and particularly who the final user of the card will be. This anonymity is less of a concern as gift cards can only be used in a limited network.

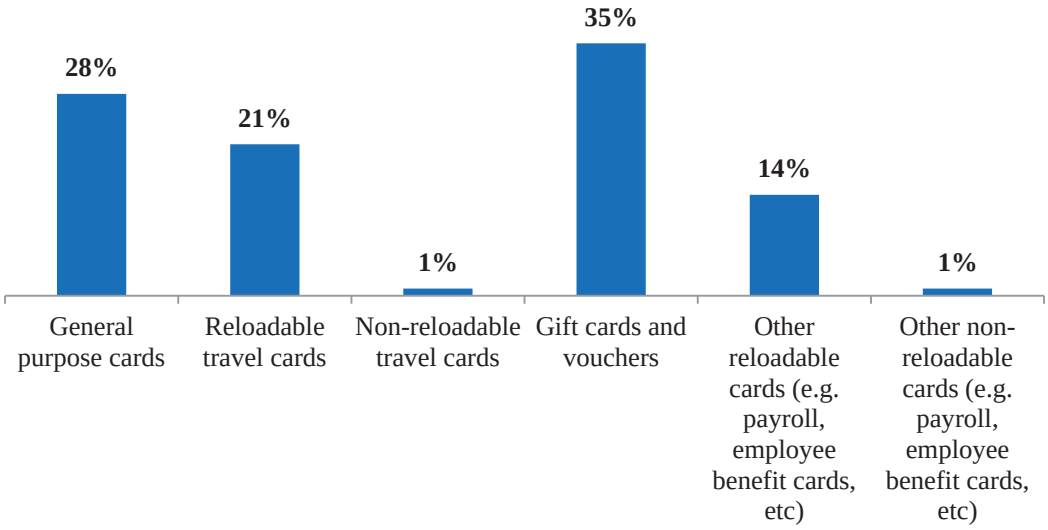
Besides these closed loop or semi-open loop prepaid cards, there are **general-purpose prepaid card**s. According to EMA, this segment represents about 12% of the total prepaid card market in Europe (2% general purpose cards, 5% travel cards, 5% corporate cards –payroll, employee benefit cards, corporate incentive cards) and 65% of transactions in value (28% general purpose cards, 22% travel cards, 15% corporate cards) International card schemes are present on that market segment too. They do not issue themselves those cards. This is the role of bank or non-bank e-money issuers.

The general purpose prepaid cards' market is very small in the European Econonic Area (source: EMA)



[102] The redemption of gift cards for cash for amounts exceeding €100 would trigger KYC obligations for their issuer under the 4AMLD.

Transaction values in the EEA by card and voucher type
(source: EMA)



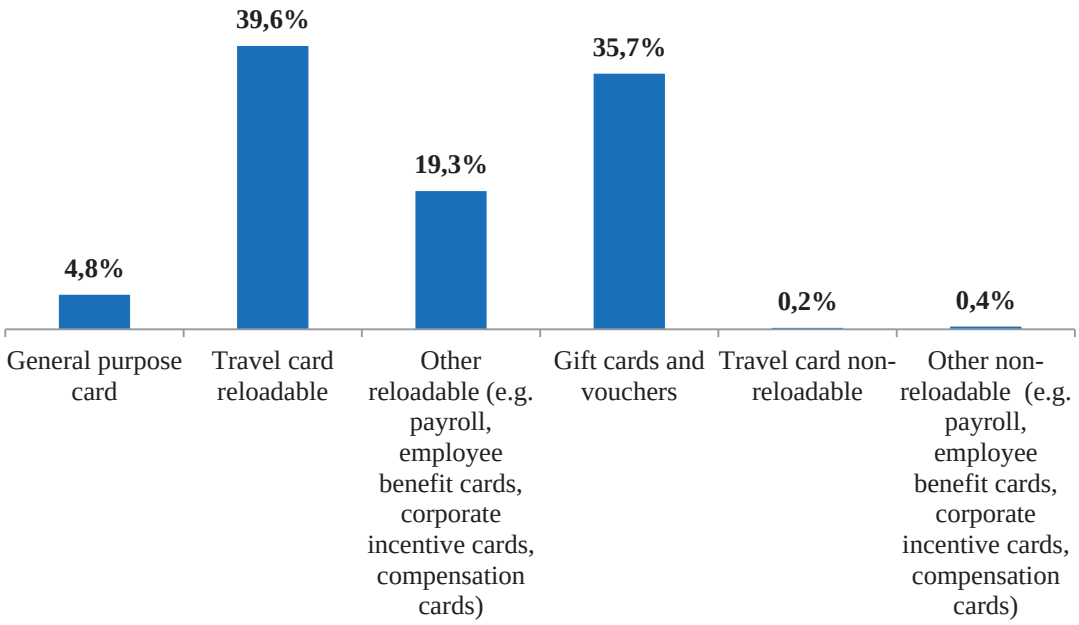
The general-purpose prepaid cards are further divided into two sub-categories: the reloadable cards and the non-reloadable cards. Many of these cards need to be activated online to become operational. This is a means to minimize theft, in particular in supermarkets and other retail stores. A code is necessary to make them operational: such a code can be attributed at the point of sale or at a later stage, when activating the card online.

(i) The general purpose non-reloadable prepaid cards, in practice, usually carry fixed amounts of €10, €20, €50 or €100. EU legislation, namely the 3AMLD, shaped the market in imposing the conduct of customer due diligence (CDD) on any buyer of a non-reloadable prepaid card with a value in excess of €250[103] (to note that Member States can double that ceiling for cards that can exclusively be used domestically). As a result, prepaid card issuers have set the maximum value for such cards at €250. In practice, all non-reloadable prepaid cards are anonymous cards with a nominal value of maximum €250. In fact, in most markets, nominal values for such cards seldom exceed €150 or £100.

(ii) The general purpose reloadable prepaid cards vary in nature and uses. There are some niche products such as travel money cards which are a substitute to paper-based travellers cheques (for instance in the UK), often for larger amounts (up to €5 000), but where customer due diligence is carried out upfront. The corporate use of such prepaid cards is currently developing, be it for the payment of salaries (e.g. for seasonal workers), the attribution of employee benefits, corporate incentive cards, or cards to cover mission expenses.

[103] Under the 3AMLD as well as the 4AMLD, Member States can double the amount of that ceiling for cards that can only be used domestically.

The truly general purpose prepaid cards' market is very small in the UK
(source: EMA)



General purpose prepaid cards programme have been developed for companies for paying perks or the salaries of seasonal workers. This avoids manipulating cash with the inherent cost and risks this entails, whilst addressing the fact that those employees might not necessarily have a bank account, or a bank account in the same currency denomination as their temporary employer. In some circumstances, those prepaid cards may be anonymous in the hands of their ultimate beneficiaries (e.g. payment of a small bonus in a form of a non-reloadable card); nevertheless, the beneficiaries are always known to the organisations dispensing them, if not to the card issuers.

Likewise, some governments pay social benefits[104] via prepaid cards with a view to reducing administration costs. The payment of social benefits is usually based on reloadable cards: the funds are paid by the public authorities to pooled accounts and then allocated to the respective beneficiaries, whose names are known in the process. Some public authorities and some non-governmental organization (NGOs)[105] today also provide prepaid cards to migrants or victims of catastrophes to allow them to immediately purchase essentials, such as food and clothing. These public authorities or NGOs act as agents to the card issuers, as far as compliance with AML/CFT requirements are concerned. In any case, the cards are in most cases physically the same. Only their functionalities vary.

Besides these specific market segments, there are truly general purpose reloadable prepaid cards. For instance, one international card scheme allows the issuance of such general purpose

[104] According to the UK Treasury, 141 local authorities in the UK use prepaid cards for the payment of social benefits (some have phased out cash offices entirely; financial help is distributed through prepaid cards).

[105] For instance, the International Committee of the Red Cross is running a program in Jordan for a value of 5.8 Mio CHF, it distributes pre-loaded bank card partially with iris scan verification in order to help for accommodation, heating and food consumption.

reloadable prepaid cards for amounts up to €20 000. The holder of such cards is however subject to customer due diligence. Major international card schemes do not allow for anonymity of reloadable cards, which means that these cards are under customer due diligence. It should be noted in this respect that the European AML/CTF legislation is more flexible as it does not require the application of customer due diligence rules where the amount put on a card over the year is less than €2 500.

Buyers of non-reloadable cards may not necessarily be banked (e.g. people on low income, students, unemployed) and will slowly get acquainted with prepaid products by purchasing them at proximity stores (supermarkets, newsagents, tobacconists). Currently such multi-purpose prepaid products can be fully exempt from any identification or verification requirement when their value is less than €250, which is the case of all non-reloadable prepaid cards issued on the territory of the EU. Many representatives of the prepaid card industry have concurred on the fact that the purchase of a non-reloadable prepaid card is a first step towards further financial inclusion, as a number of buyers, once familiarised with the product, will ask for upgrading the functionalities offered by the card, opting in particular for the possibility to reload the card. According to one major card scheme, 20% of the buyers of their non-reloadable prepaid card product would ask for the card to be converted into a reloadable card, making it equivalent in many respect to a card linked to a bank account.

Some people also choose to use prepaid cards as a means to limit the risk of fraud online as their exposure is limited to the e-money amount featuring on the card. Moreover, the physical loss of a prepaid card (with a couple of hundreds euros loaded or even less) may be much less prejudicial than the loss of a credit/debit card.

International card schemes are present on all market segments and actually two major global card schemes control the overwhelming majority of the prepaid cards issued in Europe even though they do not issue themselves those cards. This is the role of bank or non-bank e-money issuers. However, the schemes define terms and conditions that issuers have to abide by. Some rules are of an AML/CFT nature and are imposed by the schemes on their clients in order to protect the former's reputation and brand, i.e. their main asset.

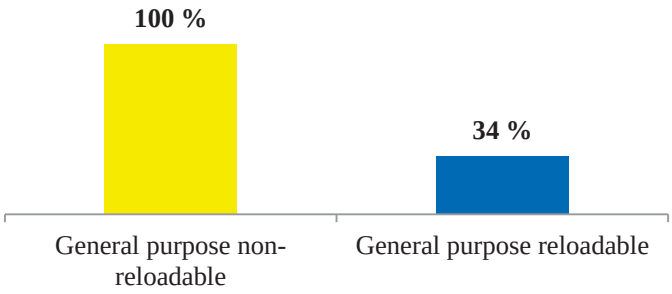
Prepaid cards are usually distributed by e-money issuers through their own branch network (in particular where these are retail banks), directly online or through retail stores (supermarkets, tobacconists, newsagents, etc.).

According to the E-Money Association (EMA), today, all (100%) general purpose non-reloadable cards are anonymous and so are 34% of the reloadable cards. The remaining 66% of the reloadable cards are subject to full CDD, meaning identification and verification of identity, at the outset, from the 1st euro. This would mean that about 57% of the general purpose cards on the market in terms of transactions value is of an anonymous nature. On the basis of an estimated prepaid card market size of €19.3 billion[106] in 2014, the yearly value of

[106] €16 billion in the euro-zone + €3.3 billion for the UK, the second biggest national market after Italy

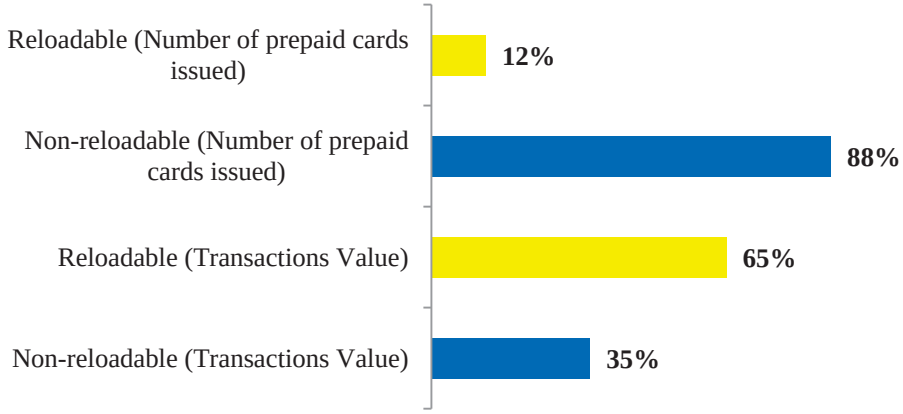
anonymous general purpose reloadable and non-reloadable cards would amount to about €5.4 billion.

Anonymous prepaid cards by categories in the EEA (source: EMA)



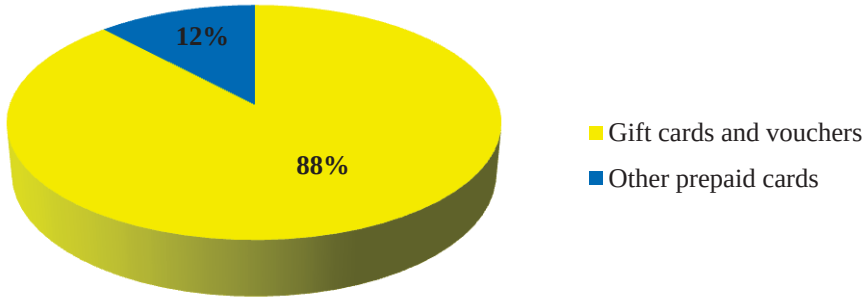
The different types of prepaid cards in the European Economic Area (EEA)

Reloadable and non-reloadable prepaid cards in the EEA (source: EMA)



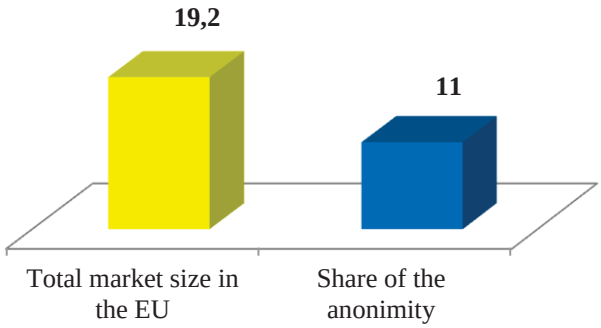
Volume of cards and vouchers in the EEA by type of function

Gift cards and vouchers represent a large majority of the prepaid cards' market in the EEA (source: EMA)

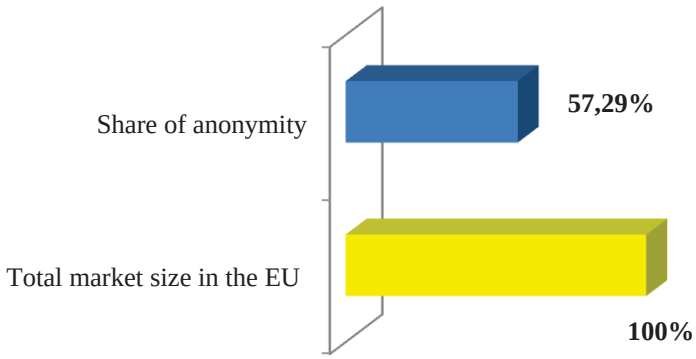


The share of anonymity is still important in the prepaid cards' market in the EEA

Anonymity in terms of transaction value in the general prepaid cards' market (€billion)
(source: EMA)



Anonymity in terms of transaction value in the general prepaid cards' market



What is the business model for prepaid cards?

Card schemes such as Visa, MasterCard, AMEX or domestic card schemes provide their cards to bank or non-bank e-money issuers, which set the parameters of the use of the card and are subject to AML/CFT requirements. The cards are then sold by those e-money issuers sometimes directly on the internet or via e-merchants and, in the brick-and-mortar environment, via banks or retail stores such as supermarkets, tobacconists, newsagents, etc. Channels of distribution of prepaid cards vary according to jurisdictions and brands.

The revenue generation depends on the type and function of the prepaid card.

- For small gift cards, the purchaser of the card will pay an upfront fee (which will be shared between the distributor, the issuer and the scheme, if distinct from the issuer).

- For general purpose reloadable cards, the revenue is generated by a fee on use and until now for part on the 'float'. However, as prepaid cards are covered by the EU Interchange Fee Regulation that has recently entered

into force, the margins on such products are likely to decline. There may therefore be a race for volume which might favour major e-money issuers and their corresponding distribution networks.

- Corporate prepaid cards seem to be an expanding segment: corporates distribute prepaid cards to their employees to cover their mission expenses, or even to pay their salaries, perks or benefits. The use of such cards generates savings for corporates which are therefore ready to pay a certain amount for that convenience.

iii. Current legislation in the EU

Issuers of prepaid instruments are covered by EU legislation, namely by the Second Electronic Money Directive and the 3AMLD to be replaced by the 4AMLD as of July 2017. Card schemes and distributors of prepaid instruments are outside the scope of those Directives.

E-money issuers are required to comply with the 'know-your-customer' requirement and apply, where need be, CDD to the card holders.

From the 3rd to the 4th AMLD, besides the stricter threshold applied to reloadable cards, the prepaid card can exclusively be used to purchase goods and services, which means that person-to-person transfers between holders of the same type of prepaid cards will no longer be allowed. Furthermore, the 4AMLD prescribes that the payment instrument benefiting from a CDD exemption cannot be funded with anonymous electronic money: funding can be made via a bank transfer or a debit or credit card payment, or in the form of a cash payment at the point of sale of the card.

One major international card scheme already applies and imposes a more stringent AML/CTF policy than the EU legislation on prepaid card issuers using its brand and products. This is in particular the case for reloadable cards for which anonymity is precluded by this card scheme, whereas the 3rd and the 4th AMLD allow Member States to be somewhat more flexible, if they so wish.

It should be underlined that individual Member States can go beyond the requirements of the EU AML/CTF legislation, if they so wish, in the respect of the Treaties and of other legislations, e.g. on data protection or on payment services (Spain for instance requires the identification at the first euro for every user of any prepaid card product). The risk-based approach enshrined in the 4AMLD would even justify the adoption by a given Member State of appropriate additional measures based on its own risk assessment of the threats it may face. However, short of a common European approach, depending on the threats and the responses adopted, in an integrated Single Market, an individual action of a Member State could rapidly become ineffective. If a given Member State decided to ban the issuing of anonymous prepaid

cards on its territory, nothing would prevent its citizens to buy them from a neighbouring Member State. This is also why for the first time the 4AMLD foresees the conduct of a supra-national assessment of money laundering and terrorist financing risks or threats at EU level, as this would be more effective in many instances than the individual action of a Member State.

iv) Current legislation in the United States

In the United States, in comparison, the banks are the main issuers of prepaid cards and are covered by the Customer Identification Program (CIP) "rule", set forth in Section 326 of the USA Patriot Act. This rule requires a bank to obtain information in order to form a reasonable belief regarding the identity of each "customer", including, at a minimum, name, date of birth, address and tax identification number. Moreover, it obliges a bank to establish risk-based procedures to verify the identity of new customers. To determine if these requirements apply to the purchasers of prepaid cards, the issuing bank should first determine whether the issuance of a prepaid card results in the creation of an account. If it is the case, the CDD measures apply.

The American authorities are also strengthening the legislation in order to lift anonymity regarding the general purpose prepaid cards. In a recent Interagency Guidance to Issuing Banks[107], the Board of Governors of the Federal Reserve System has made more precise the application of the "CIP rule". The guidance clarifies that an American bank should apply its CIP (and consequently CDD lifting the anonymity) to the cardholders of certain prepaid cards issued by the bank. In particular, the issuing of a general purpose reloadable prepaid card "creates a formal banking relationship and is equivalent to opening an account". As a consequence, the anonymity is lifted from the 1st euro for this type of prepaid cards in the United States. On the other hand, the American authorities consider that the issuing of non-reloadable general purpose prepaid cards does not "create a formal banking relationship". It leaves room here for anonymity for these cards.

The American way of thinking is not dissimilar to the proposed Option F. Nevertheless, this option represents much less compliance costs for the American issuers as they are almost only banks which are used to perform CDD measures (or take responsibility as a third-party program manager is treated as agent of the bank for purposes of the CIP rule) than it would in the European Union. The two different market structures explain the different policy options from the regulators.

[107] Board of Governors of the Federal Reserve System, "Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Access Cards" – 21 March 2016 – pages 1 to 5

i) FATF Reports regarding new means of payment, including prepaid cards

Already in 2010, the FATF typologies report "Money Laundering using New Payment Methods" described 18 cases of money laundering using prepaid cards: "*Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPMs for money launderers*".

A more recent 2013 FATF report "Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services"[108] described the ML/TF risks deriving from anonymity and the ability to use prepaid cards in non-face to face environments as follows:

> *"As with many banking methods, NPPS can allow for non-face-to-face business relationships. Depending on their characteristics, NPPS can be used to quickly move funds around the world, to make purchases and access to cash (both directly and indirectly) through the ATM network. The absence of face-to-face contact may indicate a higher ML/TF risk situation. If customer identification and verification measures do not adequately address the risks associated with non-face to face contact, such as impersonation fraud, the ML/TF risk increases, as does the difficulty in being able to trace the funds.*
>
> *For prepaid cards, the risk posed by anonymity (not identifying the customer) can occur when the card is purchased, registered, loaded, reloaded, or used by the customer. The level of risk posed by anonymity is relative to the functionality of the card and existence of AML/CFT risk mitigation measures such as funding or purchasing limits, reload limits, cash access, and whether the card can be used outside the country of issue. Prepaid cards can be funded in various ways with different degrees of CDD including through banks, the Internet, at small retail shops, or at ATMs. While funding via a bank account or through the Internet normally starts from an account or a payment instrument whose holder has been identified, cash funding or funding through other NPPS is possible and can be fully anonymous. In addition, prepaid cards can easily be passed on to third parties that are unknown to the issuer..,".*

More specifically in the context of TF risks associated with prepaid cards, the 2015 FATF report "Emerging Terrorist Financing Risks"[109] notes that:

"*Prepaid cards are replacing travellers' cheques as a method of moving money offshore. In terms of TF risk, these cards can be loaded domestically via cash or non-reportable electronic methods and carried offshore inconspicuously with no requirement to declare their movement across the border. On arrival in a high-risk country or transit country for TF, the funds are then converted back to cash through multiple offshore ATM withdrawals, restricted*

[108] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

[109] http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

only by ATM withdrawal limits. Once a loaded card has been carried offshore, funds are accessible with minimal chance of detection.

> *Prepaid cards providers that fall below AML/CTF regime thresholds are not subject to customer due diligence requirements. This can make it difficult to link a card back to an individual. Further, some of these systems allow multiple cards to be linked to common funds, allowing a third party to load funds using one card, while overseas beneficiaries access funds using a separate linked card. Additionally, any person can access the value stored on these cards with the accompanying PIN allowing for the cards to be sent to third parties more easily and securely than cash. Furthermore, some prepaid cards provide the possibility of person-to-person transfers."*

Cases study with the different options regarding anonymity

	€500 prepaid card (face-to-face)	€500 prepaid card (online)	€200 prepaid card (face-to-face)	€200 prepaid card (online)	€100 prepaid card (face-to-face)	€100 prepaid card (online)
Current Option - thresholds at €250	✔	✔	✗	✗	✗	✗
Option C - Eliminating anonymity for the online use of prepaid cards (reloadable and non-reloadable), the thresholds remain the same	✔	✔	✗	✔	✗	✔
Option D - Minimising anonymity by reducing the current thresholds from €250 to €150 (for reloadable and non-reloadable prepaid cards)	✔	✔	✔	✔	✗	✗
Combined Options C & D	✔	✔	✔	✔	✗	✔
Option E - SDD below the thresholds (identification) at the 1st €, delayed verification of identity, no change in the existing thresholds	✔	✔	○	○	○	○
Option F	✔	✔	✔	✔	✗	✔

✗ Anonymity ✔ No anonymity ○ Light anonymity

ANNEX 6: FIUs

FATF Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems (Version agreed at Plenary Meeting of FATF-XXVII (October 2015))

Recommendation 29 – Financial Intelligence Units (FIU)

"(…)

29.3 The FIU should:*

(a) in addition to the information that entities report to the FIU, be able to obtain and use additional information from reporting entities, as needed to perform its analysis properly; and

*(b) have access to the widest possible range** of financial, administrative and law enforcement information that it requires to properly undertake its functions.*

** In the context of its analysis function, an FIU should be able to obtain from any reporting entity additional information relating to a suspicion of ML/TF. This does not include indiscriminate requests for information to reporting entities in the context of the FIU's analysis (e.g., "fishing expeditions").*

*** This should include information from open or public sources, as well as relevant information collected and/or maintained by, or on behalf of, other authorities and, where appropriate commercially held data."*

International standards on combating money laundering and the financing of terrorism & proliferation (the FATF Recommendations – version updated October 2015)

Interpretative note to Recommendation 40 (Other forms of international cooperation)

"*A. PRINCIPLES APPLICABLE TO ALL FORMS OF INTERNATIONAL COOPERATION*

(…)

Unduly restrictive measures

2. *Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:*

   (a) the request is also considered to involve fiscal matters; and/or

   (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or

   (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or

   (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.

ANNEX 7: MECHANISMS FOR TIMELY ACCESS TO INFORMATION ON HOLDERS OF BANK AND PAYMENTS ACCOUNTS

1. Minimum information that should be available through the mechanism containing information on the identity of holders of bank and payment accounts

In order to reach the objective, ideally, the minimum information that should be available through the mechanism would encompass the following static[110] elements:

- Client - natural persons: a unique identification number (e.g. National Identification Number) or the identification data required under national AML/CFT law
- Client - legal persons and arrangements: a unique identification number or the identification data required under national AML/CFT law
- All IBAN bank or payment accounts of the client: the IBAN[111] number (available for all EU bank and payment accounts)
- Proxy holders on the client account: same type of data as for the client
- Beneficial owners of the clients: a unique identification number or the identification data required under national AML/CFT law
- Date of account opening and closing

All these individual elements should be useable for performing a search query.

The retention period (for maintaining the data available in the system after closing of the account) should be aligned to the existing retention period of article 40 of the 4AMLD.

[110] Including "living" data in the mechanism, such as the balance of the accounts, transaction information etc…would be technically very complex (as this would have to be permanently updated in order to be relevant), and can be obtained anyway via a targeted bilateral contact with the concerned financial institution.

[111] The International Bank Account Number (IBAN) is an internationally agreed system of identifying bank and payment accounts across national borders to facilitate the communication and processing of cross border transactions with a reduced risk of transcription errors. The IBAN consists of up to 34 alphanumeric characters, comprising a country code, two check digits and a long and detailed bank account-number (containing a.o. the national bank number and client account number).The IBAN is sufficient to identify an account for home and foreign financial transactions in SEPA countries. By being able to identify the holder of an IBAN account, the FIUs will then also be able to identify the other (non-IBAN) accounts of this person (e.g. a financial instruments trading account), as these other accounts cannot exist if they are not linked to an IBAN account.

3. Sample[112] overview: hypothetical annual costs for FIUs and the financial sector linked to blanket requests (costs[113] in €)

Member State	FIUs: duration to send the request (in minutes)	Financial institutions: duration to examine and answer to the request (in minutes)	Total number of suspicious transaction reports (STRs)	Total number of financial institutions to be contacted by the FIU	Labour cost: hourly rate (in €)	Total costs for FIUs: hypothesis of batched request[114]	Total costs for FIUs: hypothesis of separate request per financial institution[115]	Total cost for the financial sector to examine and reply to the requests
Cyprus	5	10	510	70	15,8	668,1	46 767	93 534
Latvia	5	10	26.003	68	6,6	14 301,65	972 512,2	1 945 024,4
Hungary	5	10	7.177	175	7,4	4 377,97	766 144,75	1 532 289,5
Belgium	5	10	18.673	125	39	60 687,25	7 585 906,25	15 171 812,5
Italy	5	10	37.043	729	28,3	87 051,05	63 460 215,45	126 920 430,9
Netherlands	5	10	118.559	244	34	335 521,97	81 867 360,68	163 734 721,36
Germany	5	10	11.042	1805	31,4	28 819,62	52 019 414,1	104 038 828,2

Data source: based on latest available statistics from Eurostat (Labour cost annual data of 2015; and Statistical Working Papers, "Money Laundering in Europe, edition 2013) and the European Central Bank, Payment Statistic Relevant Institutions in Q4 2014)

[112] Due to lacking information on all the relevant parameter for all Member States, a representative sample is given.

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

[114] In case a request can be processed through 1 single batch, grouping all concerned financial institutions, the frequency of the activity is equal to the number of suspicious transaction reports. This hypothesis would only be realistic if the FIU has put in place a secured electronic channel (such as for example an encrypted communication channel) with all the concerned financial institution, allowing for such batched processing.

[115] In case each request has to be processed separately for each financial institution concerned, the frequency of the activity is equal to the number of suspicious transactions x the number of financial institutions to be contacted.

4. Overview: EU Member States having or putting in place automated centralised mechanisms allowing for the identification of holders of bank and payment accounts

Member State	Status	Type of mechanism	Access by FIU to the register	Access to the register for other (law enforcement) authorities	On-off cost in €[116] (creation)	Yearly recurring cost in €[117] (maintenance)
A	Foreseen in 2016	Unknown	No	Courts and public prosecution authorities only	800.000	240.000
B	Operational	Register	No	Tax authorities only	1.000.000	600.000
C	Foreseen begin 2017	Electronic information system	Yes	Judicial authorities (courts, Prosecutor's Office, investigative bodies), Tax authorities	250.000	Unknown
D	Operational	Register	Yes	Yes, other competent authorities	250.000	Unknown

[116] Figures are rounded

[117] Figures are rounded

E	Foreseen	Register	Yes	a.o. the police	Unknown	Unknown
F	Operational	Data retrieval system	Yes	Public prosecutor	1.200.000	480.000
G	Operational	Register	Yes	Tax authorities, Customs Authorities, other competent authorities	Not given	Not given
H	Operational	Database	Yes	Law enforcement agencies and prosecutors	Unknown	Unknown
I	Operational	Register	Yes	Law enforcement authorities	Unknown	3.000
J	Foreseen	Register	unknown	unknown	Unknown	Unknown
K	Operational	Register	Yes	Prosecutor General	280.000	40.000

L	Operational	Register	Yes	Tax authorities, other law enforcement authorities	Unknown	Unknown
M	Operational	Register	Yes	Other national authorities	170.000	250.000
N	Foreseen in 2016	Register	Yes	Law enforcement authorities through the FIU and with a prior authorization of judge or public prosecutor	Unknown	Unknown
O	Foreseen	Data retrieval system (reference portal)	No	Unknown	Unknown	Unknown
P	Operational	Indirect national register	Yes	Tax authorities, police, law enforcement authorities	Unknown	Unknown

Source: information received from Member States in reply to questionnaire

ANNEX 8: DISCARDED OPTIONS

Improving the effectiveness of the EU policy towards high-risk third countries by providing for a harmonised approach at EU level with respect to enhanced due diligence measures to be applied by Member States and obliged entities.

1 **Include the FATF list of enhanced customer due diligence measures in the EU framework as examples of mitigating measures Member States and obliged entities may apply when dealing with high-risk third countries designated by the Commission.**

This option will consist in including in an Annex to the Directive the list of ECDD measures as mentioned in paragraph 20 of the Interpretative Note 10 of the FATF. This list will replicate the 7 measures presented as examples of ECDD measures that could be applied by obliged entities. On this basis, obliged entities will be asked to apply at least one of the measures provided in the Annex to business relationships they conduct with high-risk third countries.

This option A is currently implemented by all stakeholders and a purely illustrative list of ECDD would have a limited impact on the approach towards high-risk third countries. The inclusion of this list in the EU framework would only be a confirmation of current practices.

2. Include the FATF list of enhanced customer due diligence in the EU framework as well as additional ECDD specifically designated at EU level

Under this option, ECDD will be those defined at FATF level completed by some proper EU ECDD measures, such as systematic reporting below a specific threshold for instance.

Imposing such obligations to obliged entities may create disproportionate burden on their activities. In addition, it would be difficult to find a common approach to define the right criteria or threshold to trigger these additional measures, since it would depend on the size and the nature of the business that may differ from one Member State to another.

3. Include the FATF list of countermeasures in the EU framework, and require from Member States and obliged entities to apply all the set of countermeasures when dealing with high-risk third countries

Countermeasures have stronger effects than ECDD measures and may have an impact on the business activity of an obliged entity. Imposing a complete implementation of counter-measures when dealing with high-risk third countries may, here again, have an impact on the proportionality of the EU policy against third countries and may be in contradiction with the risk based approach.

Increasing the transparency of virtual currency transactions / linking transactions to an identity

1. **Prohibit the use of VCs in the EU (in payments where at least one party to the transaction is an EU resident)**

This option would achieve the objective at the highest cost in terms of digital innovation and progress. It would also contain a self-selection/screening mechanism that authorities can exploit using advanced data/big data analytics as normal users will refrain from

using VCs once their use is made illegal, whereas criminals will continue their use of VCs as long as they present some advantages over alternatives (such as banknotes).

2. **Lift VCs' anonymity through the regulation of miners**

   This would imply identifying who they are, registering them and monitoring their activity. As for users, their high number, their localisation (mostly in China) as well as the global scale of mining, makes it nearly impossible to enforce. More prominently than for users, there is a high risk to stifle innovation as miners are an essential cog of the market and any use of the technology. Finally, regulating miners only would not be a suitable solution leaving a vast majority of the market under anonymity.

Reducing the misuse of anonymous prepaid instruments by further reducing the exemption regime for anonymous prepaid cards under the 4AMLD

1. **Applying absolute limits on the value that can be uploaded on a prepaid card**

   There is no absolute cap in EU legislation or, to the Commission's knowledge, in Member States' laws (with the exception of France where a draft law addressing this issue is before the French Parliament), on the amount that can be placed on a prepaid card. In practice, the AML/CFT thresholds have defined a market cap on non-reloadable cards at the level of the threshold for CDD application (€250 for European used). It is possible for a prepaid card issuer puts on the market a €1 000 non-reloadable prepaid card. However, the cardholder would have to be subject to full CDD. Such a card would no longer be anonymous.

   As far as reloadable cards are concerned, global schemes have set their own limits (for instance for one programme at €20 000 for a reloadable prepaid card). Such limits are not defined in respect of AML/CFT considerations, as in any case such cards, or their holders rather, are subject to full CDD. Such limits or lower ones have value notably for travellers' cards which today can even be multi-currency ones or for corporate cards. It should be noted that under the 4AMLD, anonymous reloadable prepaid cards will be subject to a 250€ monthly cap on reloading.

   To the extent that such cards are subject to full CDD, the need to set an absolute limit on the amount that can be linked to the card does not seem to be an imperative.

   This approach might have some relevance where prepaid cards would be issued in foreign countries whose AML/CFT rules might not up the FATF standards. However, applying an absolute limit to cards issued in the EU or the EEA does not imply that a similar approach would be followed by foreign jurisdictions. This approach has therefore not been retained.

2. **Requesting the issuing of a new card at the time of the conversion of a non-reloadable prepaid card to a reloadable prepaid card**

   The main interest for the global card schemes and prepaid card issuers in issuing non-reloadable prepaid cards reside in the industry's ability to persuade the cardholder to upgrade its card to a (more profitable) reloadable card. The conversion rate from a non-reloadable card to a reloadable card, according to a market leader, is of about 20%. However, in practice, the card in the hands of the cardholder is not changed; its functionalities are upgraded at a distance (online or at an ATM). The question is whether it would not be appropriate that the card actually be replaced and the name of the cardholder embossed on the card.

Whilst this would be a valid course of action for a payment means mimicking a classical payment card, it is of a level of detail that might be better left to national action or self-regulation by the market, rather than an intervention at EU level, as what matters from an AML/CFT viewpoint, is that the cardholder can be identified and this does not necessarily require that its name features on the card to the extent the card number is linked to the cardholder's name, and hence the latter is retrievable.

3. **Bringing retail distributors of prepaid cards/instruments in the scope of the 4AMLD or in the scope of the Second e-money directive**

Whilst performance of CDD upon the online order of a card or its purchase at a bank branch may probably not have a chilling effect on the potential buyers, as these would be familiar with such environments (bank customers) or technologically savvy (for internet users), the same reasoning might not hold for retail distribution (supermarkets, tobacconists, newsagents, petrol stations, etc.), where the buyer would be expected to hand over cash to buy a plastic card, which in many cases will only be of use once activated and after he or she will have been identified and possibly his or her identity verified. Such a procedure could have a strong psychological deterrent effect on customers.

Furthermore, where distribution takes place through supermarkets, tobacconists or newsagents as opposed to banks or post offices, other issues come up: high staff turnover in retail distribution undermines the effect of AML/CTF training, the procedures are not always understood and the timeliness of the transmission of information to prepaid instrument issuers may be an issue. The application of AML/CFT measures would also represent a heavy administrative burden particularly for small retailers with a potential consequential risk that these products would no longer be available at proximity retail stores, favouring the use of cash over more traceable means of payment.

Making the distribution network a subject to AML/CTF in the rare cases where this has been put in place, had more to do with the fact that the prepaid instrument issuer was not always established in the markets it served. In such circumstances, the temptation was there for local law enforcement authorities to treat distributors as a 'form of establishment' of the issuer from an AML/CFT viewpoint so as to receive suspicious transaction reports directly. However, such an approach is artificial as the distributors are often not in a position to detect suspicious behavioural patterns, without the assistance of the issuer.

Distributors today, with the exception of one or two Member States, are not required to conduct CDD. If the retail sector was requested to do so, this would require investment both in IT and communication equipment as well as the training of dedicated staff. This, combined with the administrative burden, would likely imply that the sales of low margin (i.e. low nominal value) prepaid cards would simply be discontinued.

<u>Improving the FIU's access to – and exchange of – information held by obliged entities</u>

1. **Establish a European FIU to coordinate, assist and support Member States FIUs**

In this option, a European FIU would be set up in order to coordinate, assist and support Member Sates FIUs in cross-border cases. The Member States FIU would still be primarily responsible for receiving STRs, analysing them and disseminate them to the national competent authority. The EU FIU would lend support to those Member States especially in maintaining and developing the technical infrastructure for ensuring the exchange of information, assisting them in joint analysis of cross border cases and

strategic analysis, and coordinate the work of Member States FIUs for cross-border cases. In case a Member States' FIU does not have the authority to implement the 4AMLD provisions with regard to access and exchange of information between EU FIUs, the EU FIU could have a remedial procedure, or ultimately carry out the necessary tasks involving cross-border cases. It could also directly receive or facilitate the reporting of STR in a home/host context, especially for those STRs reported by obliged entities operating under free provision of services. The European FIU would provide and further develop IT systems allowing exchange of information between EU FIUs (e.g. FIU.Net). It would also improve FIU cooperation by aligning internal processes (e.g. standardisation of STR).

Such a solution would overcome the current cooperation difficulties which exist between national FIUs without being too intrusive. It would also be particularly suited to an integrated EU financial market and effective in combatting money laundering and terrorist financing in the internal market. However it would require additional funds to be made available at EU level and may raise concerns among Member States about sovereignty. In addition such approach would risk jeopardising the speedy agreement on the targeted revision of the 4AMLD. Because of its operational consequences, this option would require also a precise mapping of the Member States FIUs powers and obstacles to cooperation in order to design a well-balanced and tailor-made system of cooperation. The Commission announced in its Action Plan on Terrorist Financing its intention to carry out such mapping of Member States FIUs powers and to put forward legislative proposals to remedy to obstacles in their cooperation by mid-2017. In addition it also announced its intention to look at means to support joint analysis of cross-border cases and solutions to increase the level of financial intelligence. Therefore this option was discarded pending the result of this comprehensive mapping exercise. It will be further considered in the context of the legislative proposals to be submitted by mid-2017 on further improving FIUs' operations. Such proposals would in any case complement the provisions of 4AMLD concerning the operation of Member States FIUs which would still exist under this option.

Providing FIUs (and, as the case may be, other AML/CFT competent authorities) with an efficient mechanism to get timely access to information on the identity of holders of bank and payment accounts

1. **Registries/mechanisms at Member State level, directly accessible to all European FIUs for AML/CFT purposes**

   Enabling all European FIUs to have a direct access to the mechanisms or registries in the different EU Member States, will result in a faster access to the information concerned, as FIUs will not have to go through the international counterpart-cooperation procedure (cf. article 52-57 of the 4AMLD) in order to obtain the information. However, discussions with Member States - regarding the question whether or not the Directive allows foreign European competent authorities to consult the beneficial owner registries kept in the Member States (article 30.5 (a) of the 4AMLD) – that took place during the transposition workshops on the 4AMLD revealed that this is a very sensitive issue for a number of Member States.

   This option would facilitate the timely and comprehensive identification of bank and payment accounts of a subject throughout the Union. However, it would be legally and practically much more complex and time consuming than the national option and further examination on the viability of this European option would be necessary. In that case, the Commission would not be able to formulate its proposal by Q2 2016.

Without such direct access by foreign authorities, the information will still be accessible indirectly to such FIUs, through the international cooperation procedure. In this respect, it is to be highlighted that EU cooperation between FIUs is built on efficient tools - such as the FIU.net information exchange system - and makes use of protected channels of communication (article 56 of the 4AMLD). Moreover, as the 4AMLD is a minimum harmonization directive (cf. article 5 of the 4AMLD), Member States wanting to grant foreign authorities a direct access to their national registries or systems are free to do so under their national law.

Therefore, this option was not withheld, but will not prevent Member States from allowing the aforementioned direct access to foreign authorities if they want so.

2. A decentralised mechanism at Member State level, directly accessible to national FIUs for AML/CFT purposes

This option has the advantage of being more flexible as to the type of instrument to be used to tackle the problem. However, in that case, FIUs will not be able to obtain the information concerned through one central point, and will have to launch their queries in multiple systems or search engines. Consequently, this option would not efficiently address an essential element of the problem, being the fragmentation of the information. Moreover, the consultation by FIUs of several systems – which may be created on the basis of different parameters - enhances the risk of material errors and identification errors. Therefore, this option seems unsuitable to reach the policy objective.

3. A central registry/mechanism at European level, directly accessible to all European FIUs for AML/CFT purposes

Although this option would have the advantage of allowing FIUs to directly access all relevant information across the EU through one single registry or mechanism, it would be legally and practically much more complex and time consuming than the national option, and further examination on the viability of this European option would be necessary. In that case, the Commission would not be able to formulate its proposal by Q2 2016.

Finally, this European registry/mechanism would also raise questions on the destiny or integration of the (recently created) existing national registries or mechanisms.

Based on the above, this option was not withheld.

4. Introduce an obligation to put in place a central mechanism to identify holders of payment accounts through the second Payment Services Directive (PSD2), directly accessible to national FIUs

This option would entail a modification of the PSD2 (Directive 2015/2366) instead of the 4AMLD. In that case, logically, the information stored in the registry or available through the retrieval system would be limited to the payment accounts as defined in the PSD2. This would have as a consequence that some type of bank accounts that do not qualify as payment accounts (for example savings accounts) would not be covered by the initiative, although such accounts may contain useful information allowing FIUs to build a full view on the financial situation of persons suspected of money laundering or terrorist financing.

Furthermore there also seems to be no specific added value in modifying the PSD2 instead of the 4AMLD in order to meet the policy objective concerned.

Therefore, this option was not withheld.

ANNEX 9: NON-REGULATORY OPTIONS

POLICY OPTIONS

A mapping exercise is currently being conducted within the FIU Platform to identify practical obstacles to access to, exchange and use of information as well as operational cooperation. On the basis of the outcome of this exercise, the Commission could formulate best practices to overcome these practical obstacles, and look at means to support joint analysis of cross-border cases by FIUs and enhance the level of financial intelligence.

In addition to this, the Commission is also conducting a supranational assessment of money laundering and terrorism financing risks (as foreseen under the 4AMLD). Regular risk assessments provide an appropriate general framework to detect blind spots and respond to the evolving nature and associated risks of terrorism financing, with mitigating measures that are both evidence based and tailored to the actual risks. In this respect, the Commission could formulate Recommendations to Member States (on a "comply or explain" basis) in order to mitigate identified risks.

The Commission is also deepening its engagement within international fora dealing with counter-terrorist financing in order to enhanced the need for cooperation and exchange of information on this strategic field. In particular, the Commission is closely involved in the implementation of the FATF strategy on combatting terrorist financing where the focus is primarily put on better understanding the terrorist financing risks, the accuracy and efficiency of the existing tools to identify and disrupt terrorist financing activity at international level, the promotion of more effective domestic coordination and international cooperation to combat the financing of terrorism and the adequacy of the measures taken in relation to any countries with strategic deficiencies for terrorist financing.

Regarding prepaid cards, card schemes have the ability to impose through contractual arrangements specific AML/CTF obligations on the prepaid card issuers they work with. Card schemes would have a clear interest in doing so as it would both protect their brand and reputation and prevent possibly heavy-handed regulatory options. Some card schemes have likewise offered solutions consisting in (i) excluding the use of prepaid cards in some economic sectors (e.g. hotels, car rentals), (ii) mandating the transmission of suspicious transaction reports from card issuers directly to themselves, as they could better detect an analyse possible anomalous uses of prepaid cards, which they would report in turn to FIUs, (iii) imposing geographical restrictions. However, there are serious questions regarding the proportionality and the compatibility with the Single Market of an approach that would be based both on geo-blocking and prohibition of use in some sectors, where the normal use of a card would be legitimate.

ANALYSIS OF IMPACTS OF POLICY OPTIONS

The non-regulatory option might marginally improve the situation with regard to the baseline scenario, but will not address the specific and general objectives. Furthermore, the mapping exercise currently conducted within the FIU Platform to identify a number of practical obstacles, and the supranational risk assessment deserve more in depth analysis, given their scope, and will not allow for a swift improvement of the AML/CFT framework.

As far as the non-regulatory option regarding prepaid card schemes is concerned, such card schemes are currently not 'obliged entities' under the EU legislation and are not therefore subject to AML/CFT requirements. They would therefore first need to be brought within the scope of the 4AMLD, which would be another regulatory option.

ANNEX 10: GLOSSARY

	Explanation
Beneficial Owner	Defined in Article 3(6) 4AMLD and means any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. Identifying the beneficial owner is a key element of the customer due diligence.
Custodial wallet provider	A company that hosts and manages electronic wallets for consumers/customers (payers). Payers can top up their e-wallet using various products.
Customer Due Diligence (CDD)	Customer Due Diligence is described in Chapter II of the 4AMLD. The "regular" level of CDD imposes a duty on the obliged entity to identify and verify their customers and customers' beneficial owners, to understand the purpose and nature of the business relationship as well as to conduct ongoing monitoring (more details in Article 13)
Enhanced Customer Due Diligence (ECDD)	In the case of ECDD, the obliged entity must take a number of prescribed further customer due diligence measures, albeit on a risk-sensitive basis. (see Article 18 - 20)
Fiat currency	Currency that is legal tender, i.e. a currency established as money by government regulation or law.
Financial Action Task Force (FATF)	An inter-governmental body established in 1989 by the Ministers of its Member jurisdictions and organisations. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The European Commission and 15 EU Member States are members of FATF.
Financial Intelligence Unit (FIU)	Article 32 of the 4AMLD requires the establishment of an FIU which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential ML or TF
FIU Platform	The "EU Financial Intelligence Units' Platform" was set up in 2006 by the European Commission. It gathers Financial Intelligence Units from the Member States. Its main purpose is to facilitate cooperation among the FIUs. (The FIU platform is referred to in for example Article 51)
Legal persons (or legal entities)	Any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, Anstalt, partnerships, or associations and other relevant similar activities.
Money Laundering (ML)	ML is defined in Article 1 4AMLD as follows: The following conduct, when committed intentionally, shall be regarded as money laundering: - the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity

	to evade the legal consequences of that person's action; - the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity; - the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity; - participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.
Moneyval	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Moneyval currently comprises 30 members which are subject to its evaluation processes and procedures, including the 13 EU Member States which are not members of FATF. The aim of Moneyval is to ensure that its member states have in place effective systems to counter money laundering and terrorist financing and comply with the relevant international standards in these fields.
Obliged entity / persons	Article 2 of the 4AMLD imposes obligations on credit –and financial institutions, auditors, external accountants, tax advisors, notaries and other legal professionals (when participating in any financial or real estate transaction), trust or company service providers, real estate agents and providers of gambling services. There is also an obligation on other natural or legal persons trading in goods where payment is made in cash equal to or above €10,000.
Politically Exposed Person (PEP)	The 4AMLD defines "politically exposed persons" as natural persons who are or have been entrusted with prominent public functions. (Further specifications in Article 3(9))
Predicate offence	Are criminal activities as described in Article 3(4) of the 4AMLD. The listed categories of crimes are those for which transformation of the proceeds are considered to give rise to money laundering.
Risk based approach	Under the revised FATF recommendations and the 4AMLD, the risk-based approach allows countries and obliged entities and persons to adopt a set of measures in function of the risks in order to comply with their obligations. This helps them to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way.
Simplified Customer Due Diligence	SCDD permits obliged entities to perform reduced customer due diligence measures for certain types of customer or business presenting a lower risk. (Articles 15-17)
Suspicious Transaction Reports (STRs)	A disclosure made to a Financial Intelligence Unit (FIU) by an obliged entity or competent authority having an obligation to disclose based on the suspicion of reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted.
Terrorist Financing (TF)	TF means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that

	they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism as amended by Council Framework Decision 2008/919/JHA.
Virtual currency	a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money' (ad-hoc definition, as used by the European Central Bank).