

| INCEPTION IMPACT ASSESSMENT  |  |                 |            |
|--|--|-----------------|------------|
| TITLE OF THE INITIATIVE  | Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance) |                 |            |
| LEAD DG – RESPONSIBLE UNIT – AP NUMBER   | DG JUST – B TASK FORCE FINANCIAL CRIME   | DATE OF ROADMAP | 07/04/2016 |
| LIKELY TYPE OF INITIATIVE  | Amending Directive   |                 |            |
| INDICATIVE PLANNING  | <a href="http://ec.europa.eu/atwork/pdf/planned_commission_initiatives_2016.pdf">http://ec.europa.eu/atwork/pdf/planned_commission_initiatives_2016.pdf</a>  |                 |            |
| ADDITIONAL INFORMATION   |  |                 |            |
| <b>This Inception Impact Assessment is provided for information purposes only and can be subject to change. It does not prejudice the final decision of the Commission on whether this initiative will be pursued or on its final content and structure.</b> |  |                 |            |

| A. Context, Subsidiarity Check and Objectives   |
|---|
| <b>Context</b>  |
| <p><b>Existing legal framework</b></p> <p>On 20 May 2015 a new framework on anti-money laundering and countering 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)<sup>1</sup> and consist of:</p> <ul style="list-style-type: none"> <li>(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</li> <li>(ii) Regulation (EU) 2015/847 on information accompanying transfers of funds.</li> </ul> <p>The transposition date for the 4AMLD and the entry into force of the Funds Transfers Regulation (FTR) is 26 June 2017. Consequently, the transposition is ongoing in the vast majority of Member States.</p> <p><b>Recent events, urging for a swift political/legislative response by the EU</b></p> <p>Following the recent terrorist attacks and taking into account conclusion Nr 8 of the extraordinary Justice and Home Affairs Council of 20 November 2015, the Commission published on 2 February 2016 a Communication to the Council and the Parliament on 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 aims at updating EU policies in line with international standards<sup>2</sup>. One of the <b>key actions</b> of the action plan concerns the <b>commitment of the Commission to present – at the latest by Q2 2016 - legislative proposals to amend the 4AMLD</b> on five specific targeted points:</p> <ul style="list-style-type: none"> <li>– enhanced due diligence measures/counter-measures with regard to high-risk third countries</li> <li>– virtual currency exchange platforms</li> <li>– prepaid instruments</li> <li>– the access of Financial Intelligence Units (FIUs) to – and exchange of – information to strengthen FIU powers and cooperation</li> <li>– the access of FIUs to centralised bank and payment account registers or electronic data retrieval systems</li> </ul> <p>These amendments will further strengthen the existing legal AML/CFT framework with regard to the abovementioned targeted issues. They should not affect the ongoing transposition.</p> <p>On February 12, the Ecofin Council called on the Commission to submit these amendments as soon as possible</p> |

<sup>1</sup> 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.

<sup>2</sup> FATF standards, a.o. those regarding Financial Intelligence Units and high-risk countries.

and no later than the second quarter of 2016.

## Issue

While the recent amendment of the EU AML/CFT framework presents a major step forward in the prevention of AML/CFT in accordance with the 2012 FATF standards, recent terrorist attacks have shown that further steps to improve the framework on the prevention and fight against the financing of terrorism can be taken. The FATF convened a special plenary meeting on terrorist financing in December 2015, in order to determine further actions to strengthen the fight against terrorist financing.

The **main drivers, the issue and problem to be tackled** can be summarised as follows:

(i) **Different approaches between Member States towards high-risk countries create weak spots** which can be exploited by terrorists to channel funds in and out the EU financial system. According to article 9 of the 4AMLD, the EU will have to identify third countries with strategic deficiencies<sup>3</sup> in their AML/CFT framework ("high-risk third countries"). Article 18 of the 4AMLD states that obliged entities need to apply enhanced due diligence measures<sup>4</sup> towards entities located in such countries. To date, Member States determine at national level the type of enhanced due diligence measures to be taken towards high-risk third countries.

(ii) **The use of virtual currencies is more difficult to trace.** This can create opportunities for terrorist organisations to transfer money into the EU financial system with a certain degree of anonymity. Virtual currency transfers are currently not monitored in any way by public authorities within the EU.

(iii) **Anonymous prepaid cards can be used by terrorists** to finance part of their logistics. This was notably the case in the Paris attacks. An appropriate and carefully balanced response needs to be provided to address this issue, as at the same time, prepaid instruments also present a social value (financial inclusion, pay out of social benefits, etc.) and provide opportunities for consumers.

(iv) **Divergent interpretations of international standards** or fragmentation as regards the competence, powers or cooperation of FIUs hamper their good functioning. Especially in cases involving terrorism financing, information must flow quickly without undue delays. FIUs play an important role in identifying the financial operations of terrorist networks across borders and in detecting their financial backers. International standards now emphasise the importance of extending the scope of and the timely access to information available to FIUs, in order to further enhance their effectiveness and efficiency.

(v) **Delayed access to information by FIUs** on the identity of holders of bank and payment accounts hampers the detection of transfers of funds relating to terrorism. National data allowing the identification of bank and payments accounts belonging to one person is fragmented and therefore not accessible to FIUs in a timely manner. Although certain Member States have already put in place centralised registers or retrieval systems (as encouraged in recital 57 of the 4AMLD), there currently exists no obligation at EU level to do so. Having such a centralised register or central retrieval system in all Member States would provide direct operational support to FIUs and further enhance their effectiveness and efficiency.

Some Member States have already indicated that they intend to take national measures to fill the gaps revealed by the recent terrorist attacks, which will **create an unlevel playing field between Member States in case nothing is done at EU level.**

The **affected stakeholders** are:

- Issue (i): in theory all obliged entities under the 4AMLD that are active in high-risk third countries, but in practice this almost exclusively concerns credit and financial institutions active in those countries – measures will consist in putting in place and applying procedures on enhanced due diligence measures to be taken when doing business with entities in high-risk third countries.
- Issue (ii): virtual currency exchange platforms and their AML/CFT supervisors – measures for platforms will consist in putting in place a framework to comply with national AML/CFT legislation (transposing the 4AMLD). Supervisors will have to extend the scope of their supervision to such platforms.
- Issue (iii): issuers of prepaid instruments – issuers may have to apply customer due diligence measures in situations which currently fall under the exemption regime. Some consumers may be limited in their possibilities to pay. It should also be further examined to what extent this could affect persons benefiting from social pay outs conducted through anonymous prepaid cards (which will depend on how the policy solution is constructed).
- Issue (iv): FIUs and obliged entities: FIUs will be able to request information on ML/TF from any obliged entity under the 4AMLD.
- Issue (v): FIUs and public authorities: public authorities that currently do not have a mechanism for

<sup>3</sup> For example no or inadequate regulations and supervision of financial institutions, obstacles to international cooperation by administrative authorities or judicial authorities, absence of an FIU or equivalent mechanism etc...

<sup>4</sup> i.e. specific measures to be taken by obliged entities such as financial institutions to mitigate higher risk situations.

identifying bank and payment account holders will have to set them up, and grant FIUs access to these systems.

### Subsidiarity check

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

EU action in this area is in line with the **subsidiarity principle** as it ensures a level playing field across the EU - with entities in all Member States subject to a consistent set of AML/CFT obligations - EU action will provide better results than could be achieved by a response at Member State level only. As stated above, the FATF is currently also examining which further actions can be taken to strengthen the fight against terrorist financing. 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.

As massive flows of "illicit" money and terrorist financing 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 initiative aims at providing a harmonised approach to swiftly strengthen the EU's existing framework for the prevention of terrorist financing on a limited number of identified subjects. The identified targeted measures as set out in this inception impact assessment will be limited to what is necessary in order to attain the objectives, and therefore comply with the principle of **proportionality**.

### Main policy objectives

The **objective** of the initiative is to **swiftly reinforce the EU framework on the prevention of terrorist financing by:**

- (i) Improving 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 put in place by Member States
- (ii) enhancing transparency related to anonymous virtual currency, by imposing AML/CFT obligations on virtual currency exchange platforms
- (iii) reducing the misuse of anonymous prepaid instruments by further reducing the exemption regime for anonymous prepaid cards under the 4AMLD
- (iv) clarifying the powers of and cooperation between FIUs by ensuring that EU law is aligned with the latest international standards on AML/CFT in this field
- (v) providing FIUs with an efficient mechanism to get timely access to information on the identity of holders of bank and payment accounts

These measures are directly linked to the action proposed by the Commission in its Communication of 2 February 2016.

## B. Option Mapping

### Baseline scenario – no EU policy change

The existing AML/CFT framework of the newly adopted 4AMLD and FTR will be applicable and transposed by Member States into national legislation by 26 June 2017.

With regard to the identified areas under section A, and in the absence of a harmonised approach, there may still be important differences among the national measures taken by member States to fill the gaps revealed by the recent terrorist attacks. This may incite terrorists to exploit differences in national systems.

### Options of improving implementation and enforcement of existing legislation or doing less/simplifying existing legislation

The problems to be addressed largely do not occur due to insufficient implementation and/or enforcement of the existing *acquis* but relate to new emerging problems/threats. Issues (i), (ii), and (v) are not regulated by the 4AMLD and there is consensus at international level of the need to clarify and make effective FIU cooperation (iv). A planned FIU mapping exercise to identify practical obstacles to direct access to and exchange of information will not eliminate issue (v).

### Alternative policy instruments

By issuing its action plan to step up the fight against the financing of terrorism, the Commission took a commitment to the policy options put forward in its Communication of 2 February 2016.

### Different options

A modification of the existing EU legal framework by amending the 4 AMLD.

- (i) Harmonise the EU approach towards high-risk third countries**, by introducing in the 4AMLD harmonised enhanced due diligence measures to be taken by Member States towards such countries, and propose a list of possible countermeasures. Currently, the Commission is empowered to identify – by way of a delegated act - high-risk third countries according to article 9 of the 4AMLD. Such high-risk third countries have deficient AML/CFT regimes in place, and therefore constitute an important risk for terrorist financing. By harmonising the enhanced due diligence measures to be taken towards such countries at European level and proposing a list of possible countermeasures, the risk of diversion to less strict regimes is being tackled.

➤ **Possible alternatives:**

*Harmonise the EU approach towards high-risk third countries, by introducing in the 4AMLD:*

- *Option 1: a mere list of possible enhanced due diligence measures and countermeasures (i.e. Member States can pick/choose on or more measures on these lists, so the possible measures would be harmonised, but the choice would not be harmonised. This would be a lighter option);*
- *Option 2: a harmonised approach of enhanced due diligence measures and countermeasures to be taken (i.e. both sets of measures would be harmonised as regards the choice. This would be a tougher option).*

- (ii) Deal with anonymous virtual currency**, by bringing virtual currency exchange platforms under the scope of the 4AMLD (i.e. make them an "obliged entity") and supervise their compliance with AML/CFT legislation. This would constitute a first step in preventing terrorist financing through anonymous virtual currencies.

➤ **Possible alternatives:**

- *Also regulate virtual wallet providers by including them in the scope of the PSD2 or 4AMLD*
- *Regulate anonymous virtual currency by submitting virtual currency exchange platforms to a fully-fledged prudential licensing and supervision regime under the Payment Services Directive (PSD2)*

- (iii) Address the misuse of anonymous prepaid instruments** (such as prepaid cards), by further reducing the existing exemption regime linked to those instruments in the 4AMLD. As the recent Paris terrorist attacks have shown, prepaid instruments were used in the financing of these events.

➤ **Possible alternatives among others:**

- *entirely suppress all the existing exemptions for prepaid instruments foreseen in the 4AMLD,*
- *regulate other actors active in the prepaid instruments business, such as for example distributors of prepaid cards, by modifying Directive 2009/110/EC (the "e-money Directive")*
- *lower the existing thresholds applicable to reloadable/non reloadable anonymous prepaid instruments under the 4AMLD*
- *provide for the application of customer due diligence requirements at the time of activation of the prepaid instruments/in case of non-face to face use of prepaid instruments*
- *a combination of some of the alternatives listed above*

- (iv) Enhance the powers of and cooperation between FIUs, and their fast access to necessary information, by enabling them to obtain additional information from any reporting entity that is covered by the 4AMLD,**

- *by modifying the 4AMLD in order to clarify that FIUs shall have direct access to information held by obliged entities and that they are not limited to request supplementary information only from the reporting entity that filed an original suspicious transaction report (STR). This would ensure that FIUs are better equipped to collect the necessary information to assess STRs more efficiently.*

➤ **Possible alternatives:**

- *establish a single European FIU, having the right to request/obtain relevant information from*

*all obliged entities operating within the EU.*

**(v) allow for a timely identification of holders of bank and payment accounts by FIUs:**

- by modifying the 4AMLD in order to ask Member States to set up centralised mechanisms allowing the identification of the payment and bank accounts belonging to one person, and granting FIUs (and – as the case may be – other (national) AML/CFT authorities) access to such centralised mechanisms. Such centralised mechanisms could take various forms, e.g. a central banking registry or a mere central retrieval system.

➤ **Possible alternatives:**

- *to introduce centralised mechanisms allowing the identification of bank and payment accounts belonging to one person through a self-standing Directive, with a view to harmonise the access to these mechanisms for a broader group of authorities (tax authorities, police, customs, etc...) and for a broader purpose (e.g. all law enforcement purposes).*
- *to introduce such centralised mechanisms through an amendment of the Payment Services Directive (Directive 2015/2366). However, in that case, it would also be logic to limit the mechanism to payment accounts, which is only part of the accounts that are targeted by the initiative.*

**Alternative/differentiated scope**

Taking into account the fact that the objective of this initiative is to swiftly strengthen the EU's existing framework on the prevention of terrorist financing on a limited number of clearly identified subjects, this aspect does not seem relevant.

**Preliminary proportionality check**

The approach put forward is a limited and targeted modification of the 4ALMD, an existing core EU legislative instrument in the field of the prevention of terrorist financing. This constitutes the lightest way of realising the abovementioned objectives regarding the prevention of terrorist financing, and has a limited impact on stakeholders.

**C. Data Collection and Better Regulation Instruments**

**Data collection**

**Existing sources of information**

- Studies, reports, and documents published by the Financial Action Task Force (FATF) and the regional standard setting body Moneyval. Including:
  - FATF 2012 Recommendations revised in October 2015
  - Terrorist financing: FATF Report to G20 Leaders - actions taken by FATF of November 2015
  - Money Laundering through the Physical Transportation of cash of October 2015
  - FATF's Guidance for a Risk-Based Approach to Virtual Currencies of June 2015
  - FATF report on Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL), February 2015
  - FATF's Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services of June 2013
  - Mutual evaluation reports (MERs) of EU/EEA member States, in particular of Belgium, Italy, Norway and Spain (reports published between 2014 - 2015)
- Studies, reports published by the European Banking Authority, in particular
  - Opinion on 'virtual currencies' of 4 July 2014
  - Report on the application of AML/CTF obligations to, and the AML/CTF supervision of e-money issuers, agents and distributors in Europe, of December 2012
- Other studies, reports, and information including
  - Report by the ECB on "Virtual currency schemes – a further analysis" of February 2015
  - Report by the IMF on "Virtual currencies and beyond: Initial considerations" of January 2016

- Reports by the Egmont Group of Financial Intelligence Units, such as the Findings of its ISIL Project with regard to Multilateral Information Sharing Challenges, of 15 October 2015
- Report by the IMF on "Virtual currencies and beyond: Initial considerations" of January 2016
- National reports on the issues covered by the proposed amendments<sup>5</sup>
- Letter of Europol of 2 January 2016 on centralised bank account registers

### **Targeted data collection**

A targeted data collection is currently being conducted to fill a limited number of information gaps that have been identified by Commission services. Initial desk research has been based on preparatory work done in relation to the 4AMLD. The Commission already has some data from card schemes (e-money market, types of pre-paid cards, various business models...). Reliable data regarding virtual currencies, both at European and national levels, remains a challenge. Following this work, the Commission will need information and further data on:

- how national authorities collect data to detect and assess suspected terrorist activities and information on how such data are collected and used (i.e. through initial suspicious transaction reports filed by obliged entities or through information obtained following additional complementary requests) (issue iv)
- the existence and cost/benefit of national bank and payment accounts registers, or other similar centralised systems, and to what extent this information can be used by national authorities to detect terrorist financing (issue v)
- the size of the market of prepaid instruments/vouchers (issue iii), and virtual currencies (issue ii)
- to what extent virtual currencies, prepaid instruments/vouchers present characteristics which make them vulnerable to being used for or involved in terrorist financing (either directly or indirectly) (issue ii and iii), or a representative selection of Member States have taken or plan to take any measures with respect to those instruments
- where applicable, existing monitoring mechanisms and internal controls to ensure traceability of prepaid instruments along their chain as well as whether the use of the card could be limited (issue iii)
- what kind of customer due diligence measures do obliged entities apply in their business relationships with regard to transactions involving high-risk third countries (issue i).

### **Consultation approach**

In order to collect the abovementioned data, the Commission has already issued the following questionnaires/surveys:

- **December 2015: Survey Member States (FIUs and public authorities) to explore the agreed problem areas relating to terrorism financing, to seek policy views and data.** This covers:
  - how national authorities collect data to detect and assess suspected terrorist activities and how this information is used
  - mapping the existence of centralised national bank and payment accounts registers, or other similar mechanisms, such as central data retrieval systems, and to what extent this information can be used by national authorities to detect terrorist financing
  - examining the market structure and any regulatory responses at national level for prepaid instruments and virtual currencies, and the extent to which these instruments have been used in terrorist financing
  - tackling financial flows coming from high-risk third countries via enhanced due diligence measures/countermeasures
- **December 2015 – ongoing: Consult affected stakeholders on terrorist financing challenges and policy solutions:** covering:
  - the payment industry: bilateral meetings have been and are organised with all relevant actors
  - consultation with relevant virtual currencies market players: exchange platforms, wallet providers,

<sup>5</sup> For example: the UK Treasury's report 'Digital currencies: response to the call for information', published in May 2015 and the Tracfin, Countering Terrorist Financing, November 2015 [\[link\]](#).



representative association of virtual currency stakeholders

- FIUs: a questionnaire has been issued on cooperation, information exchange and access to/use of central bank registries and mechanisms
- Banking and financial sector: questionnaires on bank registers and enhanced due diligence/countermeasures have been issued;
- Europol and possibly law enforcement authorities.

Due to the political urgencies and against the background that the envisaged amendments are targeted, it is not needed to undertake a comprehensive public consultation.

#### Will an Implementation plan be established?

Yes  No

The relevant issues will be covered, as appropriate, by extending or building upon the already existing implementation plan that seeks to ensure that the 4AMLD is transposed into national legislation no later than 26 June 2017. This implementation plan was presented to and agreed with the Member States on 25 September 2015.

### D. Information on the Impact Assessment Process

This Inception Impact Assessment sets out the headlines of the proposed modifications to the 4AMLD. **Taking into account** the fact that **it concerns five limited and targeted amendments to a recently adopted Directive** on which a full impact assessment was conducted, the impact assessment should be **clearly focussed on the amendments sought** and build on earlier impact assessment work where relevant.

The work on the impact assessments builds on targeted data collection and existing information. It is worth emphasising that all five targeted amendments concern **issues that were already envisaged or discussed during the negotiations on the 4AMLD:**

- **the strengthening of FIU powers and cooperation** (p. 102-103 IA 4AMLD), the exemption regime for **anonymous prepaid instruments** (p. 100 and 112-113 IA 4AMLD), and the **harmonisation of sanctioning regimes** towards non-compliant actors (such as (counter)measures to be taken **towards high-risk third countries**) (p. 92-93 IA 4AMLD), have all been examined under the impact assessment for the 4AMLD.
- On the two other issues, discussions took place during the negotiation process. On **virtual currency exchange platforms**, there has been a proposal to include them in the scope of the 4AMLD, but the analysis was produced too late for there to be sufficient consensus in the Council to cover the matter at that time. On **central bank registers**, the discussions led to the inclusion of a recital recommending Member States to create such registries (recital 57 of the 4AMLD), but at that time, there was no sufficient consensus to make this mandatory at EU level.

The existing Inter Service Group on anti-money laundering and counter terrorist financing will, immediately after the political validation, be engaged in the work on and discuss/review the draft Impact Assessment and the proposed amendments.

### E. Preliminary Assessment of Expected Impacts

On the basis of the consultations already performed or ongoing at this moment, the preliminary assessment of expected impacts can be summarised as follows:

- **Measure (i):** further harmonisation on these measures will limit/avoid the risk of forum-shopping between less/more stringent regulations towards high-risk third countries. At EU level, this avoids the creation of gaps that could be exploited for ML/TF activities.
- **Measure (ii):** on virtual currencies, the FATF and EBA have issued recommendations that – at least - virtual currency exchange platforms should be brought within the scope of AML/CFT supervision. Nearly all EU Member States have issued warnings on the use of virtual currencies, and from the survey conducted, it appears that a significant number (27) of Member States support an EU framework on this. This initiative aims to be a first step in mitigating the recognised AML/CFT risks related to virtual currencies.

The impact of bringing virtual currency exchange platforms under the AML/CFT legislation would be quite limited for stakeholders, as it would only affect the existing platforms (which will have to bear the additional costs related to their compliance with the AML/CFT framework, in case they do not apply this framework already on a voluntary basis) and their supervisors (which will have to bear the costs for supervising those platforms. Presumably, Member States will entrust the AML/CFT supervision of these

platforms to their existing market/financial supervisors).

- **Measure (iii):** limiting the anonymity of prepaid instruments will be an incentive to use such instruments for legitimate purposes only, and will make them less attractive for terrorists and criminals. The impact for the prepaid instruments sector would essentially consist in bearing the additional cost for applying customer due diligence measures when selling prepaid instruments which currently fall under the exemption regime.
- **Measure (iv):** the clarification of the FIUs' mandate to request supplementary information from any obliged entity and have direct access to information held by obliged entities will ensure that the legislation in all Member States is aligned with international standards. This will make FIUs better equipped to collect the necessary information to assess STRs more efficiently and speed up detection of terrorist financing and money laundering activities. The obligation to make changes in this area will be on Member States/public authorities themselves.
- **Measure (v):** the timely and easy identification of all bank and payment accounts belonging to one person by FIUs (and - as the case may be – other AML/CFT authorities) will lead to a faster detection - both nationally and internationally - of suspicious ML/TF transactions, and improve preventative action in this field. This measure does not pose cost/benefit burdens on the market (centralised registers/centralised retrieval systems may in fact decrease regulation burden by avoiding numerous small/repeated requests for information).

#### **Likely economic impacts**

Taking into account the fact that the initiative is limited and targeted, the negative economic impacts should be small. On the economic gains, direct and indirect costs for Member States that are subject to a terrorist attack are generally high (damage to infrastructure, impact on the stock market and the commercial life, costs for improving national security, etc...). It is very difficult to measure the economic gains linked to the prevention of terrorist attacks or to the prevention of money laundering.

#### **Likely social impacts**

Improving preventative measures in the field of terrorist financing can limit terrorist attacks, which can have an important positive social impact.

#### **Data protection and fundamental rights**

The impact on data protection and fundamental rights will also have to be analysed further.

#### **Likely environmental impacts**

There seem to be no such impacts.

#### **Likely impacts on simplification and/or administrative burden**

The administrative burden linked to the initiative will be limited (mainly: setting up a centralised mechanism for identifying bank and payment account holders in Member States that do not yet have such a mechanism, and provide for AML/CFT supervision of virtual currency exchange platforms).

#### **Likely impacts on SMEs**

The impact of the proposed measures on SMEs active in the field of prepaid instruments and virtual currencies will depend on the chosen options, and is to be examined further when conducting the impact assessment.

#### **Likely impacts on competitiveness and innovation**

Apart from the case of virtual currencies, where the potential effects (if any) on innovation are currently not clear (cf. supra), and will depend on the chosen options, the impacts on competitiveness and innovation seem rather limited at first sight. However, this will need to be further analysed in the impact assessment.

#### **Likely impacts on public administrations**

Implementation costs for national authorities should remain limited (mainly: setting up a centralised mechanism for identifying bank and payment account holders in Member States that do not yet have such a mechanism, and provide for AML/CFT supervision of virtual currency exchange platforms).

#### **Likely impacts on third countries, international trade or investment**

The EU will have a harmonised approach on enhanced due diligence measures to be taken towards high-risk third countries, thus avoiding distortions between Member States with regard to international trade or investment.