



Brussels, 7 July 2016
(OR. en)

Interinstitutional File:
2016/0208 (COD)

10678/16
ADD 2

EF 208
ECOFIN 661
DROIPEN 121
CRIMORG 73
COTER 70
CODEC 966
IA 51

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	6 July 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2016) 224 final
Subject:	COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document 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 and amending Directive 2009/101/EC

Delegations will find attached document SWD(2016) 224 final.

Encl.: SWD(2016) 224 final



Strasbourg, 5.7.2016
SWD(2016) 224 final

COMMISSION STAFF WORKING DOCUMENT
EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT

Accompanying the document

**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 and amending Directive
2009/101/EC**

{ COM(2016) 450 final }
{ SWD(2016) 223 final }

Executive Summary Sheet

Impact assessment on a *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*

A. Need for action

Why? What is the problem being addressed?

While Directive (EU) 2015/849 presents a major step forward for the prevention of money laundering and terrorist financing in the EU, recent terrorist attacks and disclosures regarding certain deficiencies in the worldwide financial system ("Panama papers") demonstrate that further steps to improve this framework are needed. In this respect, five problems need to be addressed in relation to the financing of terrorism:

- (1) Unclear and uncoordinated customer due diligence requirements resulting in less efficient monitoring of suspicious transactions involving high risk-third countries;
- (2) Suspicious transactions made through virtual currencies are not sufficiently monitored by the authorities;
- (3) Insufficient measures to mitigate risks associated with anonymous prepaid instruments;
- (4) Limitations in ensuring Financial Intelligence Units' (FIUs) timely access to – and exchange of – information held by obliged entities;
- (5) FIUs lack access, or have delayed access, to information on the identity of holders of bank and payment accounts.

The proposed amendments also address problems linked to lack of access to updated beneficial ownership (BO) information in relation to corporate and legal arrangements.

What is this initiative expected to achieve?

The proposed amendments are expected to ensure more transparency and help competent authorities to effectively detect criminal and terrorist financing flows. The amendments should (a) ensure more legal certainty for obliged entities as regards the enhanced customer due diligence measures which need to be applied in relation to high-risk third countries, (b) improve the detection of suspicious virtual currency transactions; (c) reduce the misuse of anonymous prepaid instruments; (d) improve FIUs' access to, and exchange of, information held by obliged entities; (e) ensure swift access to relevant information on the identity of holders of bank and payment accounts to prevent and detect transactions linked to money laundering and terrorist financing, and (f) enhance transparency of beneficial ownership of corporate and legal arrangements.

What is the value added of action at the EU level?

This initiative aims to provide a harmonised approach to swiftly strengthen the EU's existing framework for the prevention of money laundering. The lack of an effective preventative legal framework in one Member State may be exploited by criminals and terrorist, and have consequences in another Member State. Therefore, it is important to have a harmonised framework at EU level.

B. Solutions

What legislative and non-legislative policy options have been considered? Is there a preferred choice or not? Why?

The Commission has considered non-legislative options such as to formulate 'best practices' to overcome the practical obstacles identified in an ongoing mapping exercise and recommendations to Member States (on a 'comply or explain' basis). However, such options should complement - rather than replace - legislative action.

A wide range of regulatory options have been considered to address the identified problems. The preferred options in the relevant areas are selected to strike a balance between achieving the objectives and the possible adverse impacts on market participants, in particular compliance costs. This options include: (i) a prescriptive list of enhanced customer due diligence measures to be applied by obliged entities in combination with an illustrative list of countermeasures, (ii) bring virtual currency exchange platforms and custodial wallet providers under the scope of the Directive in combination with the creation of a system of voluntary self-identification of virtual currency users, (iii) suppressing the anonymity for the online use of reloadable and non-reloadable

prepaid cards and a reduction of the existing threshold for anonymous prepaid cards when used face-to-face (from € 250 to € 150), (iv) a clarification of the legal obligations on FIUs as regards their access to and exchange of information held by obliged entities, (v) an automated central mechanism at national level, allowing for the identification of bank and payment accounts, and (vi) measures improving transparency and access to information on beneficial owners of corporate and legal arrangements.

C. Impacts of the preferred option

What are the benefits of the preferred option (if any, otherwise main ones)?

The preferred options will ensure more transparency and help competent authorities to effectively detect criminal and terrorist financing flows, and in particular:

- bring more legal certainty to obliged entities when dealing with customers in high risk third countries,
- tackle issues of transparency and limit anonymity for certain identified payment instruments (without wiping out the benefits that these instruments offer in their normal use),
- allow FIUs to have access to more information from obliged entities and swift access to information that identifies bank and payment account holders thus avoiding cumbersome blanket requests
- improve access by public authorities to beneficial ownership information, thus enhancing transparency of legal arrangements and corporate structures.

What are the costs of the preferred option (if any, otherwise main ones)?

Costs triggered by the proposed amendments vary significantly from one proposal to another. The proposed provision to improve the detection of suspicious virtual currency transactions and increase the transparency of such transactions would generate a cost of approximately €10 client.

Costs (e.g. for setting up automated central registries or electronic data retrieval systems, will depend on the model (one-off costs ranging from €175 000 to €1 200 000) and must be seen in the overall context of achieving more transparency and a more rapid and accurate detection of money laundering and terrorist financing. Lifting or reducing anonymity for prepaid cards implies certain costs linked to complying with the obligations in the Directive. However, most prepaid card issuers also issue non-anonymous prepaid cards, and therefore already have in place the necessary staff and IT systems to comply with these obligations.

How will businesses, SMEs and micro-enterprises be affected?

Certain businesses, such as virtual currency exchange platforms and custodial wallet providers will be brought under the Directive, which generates a certain cost, as it will put them under a supervisory regime. Lifting or reducing anonymity for prepaid cards also implies a certain costs.

Will there be significant impacts on national budgets and administrations?

For national authorities, there will be costs for setting up automated central registries or electronic data retrieval systems. The cost will depend on the model and based on input received from 5 Member States, one-off costs for such tools range from €175 000 to €1 200 000, while yearly recurring costs range from €3 000 to €600000.

Will there be other significant impacts?

No

D. Follow up

When will the policy be reviewed?

Two to four years after the adoption of Directive (EU) 2015/849 (i.e. 26 June 2019 - 26 June 2021).