Questions and Answers: Anti-money Laundering Directive

Strasbourg, 5 July 2016

The Commission has today adopted a proposal to further reinforce EU rules on anti-money laundering to counter terrorist financing and increase transparency about who really owns companies and trusts.

The adoption of the Fourth Anti-Money Laundering Directive (AMLD) in May 2015 was a major step forward in improving the effectiveness of the EU's efforts to combat the laundering of money from criminal activities and to counter the financing of terrorist activities. This Commission proposal is the first initiative to implement the Action Plan for strengthening the fight against terrorist financing of February 2016 The recent terrorist attacks and the Panama Papers revelations highlighted the need for the EU to take further measures and step up its fight against money laundering and terrorism financing.

This proposal, amending the Fourth Anti-Money Laundering Directive, intends to complement the existing preventive legal framework in place in the Union, by setting out additional measures to better counter the financing of terrorism and to ensure increased transparency of financial transactions and legal entities.

1. Tackling Terrorism Financing

How does the EU currently tackle the use of the financial system for terrorist financing purposes?

The EU has set up strong rules to combat money laundering and the financing of terrorism, to prevent the EU financial system from being misused for these purposes. The Fourth Anti-Money Laundering Directive, adopted on 20 May 2015, set high standards to ensure that credit and financial institutions are equipped to detect and take action against such risks. For instance, it introduced a requirement for Member States to put in place national registers of beneficial owners, to ensure transparency around certain ownership structures.

The swift transposition and implementation of these new rules is the first key step. Member States have committed at the level of Finance Ministers to bring forward the date for effective transposition and entry into force to end 2016 at the latest.

Given the evolving risks, the Commission is today proposing some amendments to improve the current legislative framework, and speed up some other non-legislative initiatives.

What changes does today's proposal introduce to fight terrorist financing?

The Commission proposes a number of targeted amendments to the Fourth Anti-Money Laundering Directive.

The amendments will strengthen the following points:

- Apply enhanced checks (“due diligence measures/counter-measures”) towards high risk third countries;
- Bring virtual currency exchange platforms under the scope of the Directive;
- Strengthen transparency measures applicable to prepaid instruments, such as prepaid cards, by lowering thresholds for identification from €250 to €150 and widening customer verification requirements;
- Enhance the powers of Financial Intelligence Units and facilitate their cooperation by further aligning the rules for such Units with the latest international standards;
- Give Financial Intelligence Units swift access to information on the holders of bank-and payment accounts, through centralised registers or electronic data retrieval systems.

What are Financial Intelligence Units?

They are public authorities that exist in every Member State. They collect and analyse information about any suspicious transactions spotted by banks, for instance, or any other relevant information related to money laundering or terrorism financing. If their analysis of a file raises concerns regarding

possible criminal activity, they transfer the file to law enforcement authorities for further action.

How will the work of Financial Intelligence Units in the fight against terrorism financing be facilitated?

The access of Financial Intelligence Units (FIUs) to – and exchange of – information will be enhanced in two ways:

- *by introducing centralised bank and payment account registers*: centralised registers at national level allow for identification of all national bank accounts belonging to one person, or other similar mechanisms such as "central retrieval systems". They are used by law enforcement authorities to facilitate financial investigations, including those relating to terrorism financing. The establishment of these centralised registers or electronic data retrieval systems in all Member States will rapidly provide FIUs (or other competent authorities) with information on the identity of holders of bank and payment accounts. In parallel, the Commission will look into the possibility of a distinct legal instrument to broaden the scope for accessing these centralised bank and payment account registers for other purposes (e.g. law enforcement investigations, including asset recovery, tax offences) and by other authorities (e.g. tax authorities, Asset Recovery Offices, other law enforcement services, Anti-corruption authorities). Any initiative would have to be accompanied by appropriate safeguards, in particular as regards data protection, and conditions of access.
- *by aligning the rules for Financial Intelligence Units (FIUs) with the latest international standards*: 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 access to information available to FIUs (that information is currently limited in certain Member States by the requirement that a prior Suspicious Transaction Report has first been made by an obliged entity). The Commission proposes to amend the Fourth AMLDin order to enhance the access to information available to FIU's.

What can the EU do to further address terrorist financing risks linked to high-risk third countries?

Today, the Fourth AMLD requires obliged entities, such as banks and financial institutions, to apply enhanced customer due diligence measures (i.e. extra checks and monitoring of financial transactions in order to prevent, detect and disrupt suspicious transactions) when doing business with natural or legal entities established in "high risk third countries" (see also below). However, at present, Member States are not required to include, in their national regimes, a specific list of enhanced measures and thus various regimes – stricter and less strict – exist in this field.

Harmonisation of these measures at EU level will avoid or at the least limit the risk of forum-shopping between the different Member States, thus avoiding weak spots that could be exploited by terrorists to channel their funds in an out of the EU.

The enhanced measures proposed are fully compliant with the list of such actions drawn up by the Financial Action Task Force ("FATF"). The list of countermeasures set out by FATF should also be adequately reflected in Union legislation.

How can virtual currencies be used to finance terrorism and what can we do to prevent this?

Banks and payment institutions fall under the scope of the Fourth AMLD, which requires them to comply with specific rules, such as verifying customers' identity and monitoring financial transactions. Virtual currency operators were initially not included in the scope of the Directive.

Virtual currencies are developing quickly and are an example of digital innovation. However, at the same time, there is a risk that virtual currencies could be used by terrorist organisations to circumvent the traditional financial system and conceal financial transactions as these can be carried out in an anonymous manner.

That is why the Commission proposes to bring virtual currency exchange platforms and custodian wallet providers under the scope of the Fourth AMLD, in order to help identify users who trade in virtual currencies. Bringing these two actors under the Fourth AMLD and making them "obliged entities" will ensure better controls, ensuring that they apply customer due diligence and contribute to preventing money laundering and terrorist financing.

What is the difference between a virtual currency exchange platform and a virtual wallet provider?

Virtual currency exchange platforms can be considered as 'electronic' currency exchange offices that trade virtual currencies for real currencies (or so-called 'fiat' currencies, such as the euro). On the other hand, virtual currency custodian wallet providers hold virtual currency accounts on behalf of their customers (by providing virtual wallets from which payments in virtual currencies can be done or received). In the 'virtual currency' world, they are the equivalent of a bank or payment institution

offering a payment account.

Why not just ban virtual currencies?

Whilst several jurisdictions in the world, including some European Union Member States and the European Banking Authority, have issued warnings about the risks that virtual currencies may entail, none have actually banned them. Virtual currencies are often considered as a useful tool for international payment transfers, low cost money remittance and close to instantaneous payments. To date, virtual currencies represent an innovative but rather small market. The European Central Bank in its last report on virtual currencies (February 2015) concluded that virtual currencies entail certain risks but do not at this point in time pose a threat to financial stability due to their still limited size – around 70,000 transactions are made daily on virtual currency platforms, worth around €40 million. Obviously, responsible authorities will continue to monitor the developments in this area.

What are the risks linked to pre-paid cards, and how can they be tackled?

Whilst the Commission fully acknowledges that prepaid instruments can have a social purpose and are beneficial for many citizens, including for those who are economically vulnerable or financially excluded, it is also aware of the risks stemming from the anonymity of some of these cards. For this reason, the Commission proposes to amend the Fourth AMLD to minimise the anonymous use of these products.

Given the risk of terrorist financing, the Commission proposes to minimise the use of anonymous payments through pre-paid cards, by lowering thresholds for identification from €250 to €150 and widening customer verification requirements for payments 'on site'. More stringent provisions will apply for prepaid cards used on the internet so that anonymous use will not be possible online. Proportionality has been taken into account, with particular regard paid to the use of these cards by financially vulnerable citizens.

What about prepaid cards issued outside the EU, that are used in the EU?

While the use of anonymous prepaid cards issued in the EU is essentially limited to the EU territory only, this is not always the case with similar cards issued in third countries. The proposal contains a provision to ensure that anonymous prepaid cards issued outside the EU can be used in the EU only where they can be considered to comply with requirements equivalent to those set out in EU legislation. This means that banks will carry out their checks and will have to refuse payments made with cards from countries that do not have sufficiently high anti-money laundering standards.

What other non-legislative actions will the EU take in the fight against terrorist financing?

a) Support work done by Financial Intelligence Units

The EU will continue delivering operational support to Financial Intelligence Units (FIUs). FIUs in Europe exchange information and identify money laundering and terrorist finance activities by matching information on suspected transaction reports through a decentralised IT system called FIU.net. The FIU.net network was integrated into Europol on 1 January 2016, helping police authorities to fight against terrorist financing.

b) Tackling obstacles to information exchanges between FIUs

A planned mapping exercise among FIUs to identify practical obstacles to access to and exchange of information will be advanced and accelerated. FIUs are also expected to interact closely with other enforcement authorities. In this context, the Commission will also further look at means to support joint analysis of cross-border cases by FIUs and solutions to enhance the level of financial intelligence. The EU FIU Platform – representing Member States FIUs - will provide the results of its analysis before the end of 2016. The Commission will propose new initiatives by mid-2017 to remove the identified obstacles and increase financial intelligence.

c) Conducting a supranational risk assessment of money laundering and terrorist financing risks, in line with the provisions of the Fourth Anti-Money Laundering Directive

In order to avoid blind spots and respond to the evolving nature of terrorism financing, the EU will put in place a framework to analyse terrorism financing risks in a broader perspective. The aim is to analyse the risks affecting the internal market and propose mitigating actions, including Recommendations to Member States (on a "comply or explain" basis) to address such risks. The Commission has already designed the methodology for this assessment and started the analysis process. Such a framework should allow the Commission to develop, in addition to Recommendations to Member States, new policy initiatives at EU level which are both evidence-based and tailored to the actual risks.

2. **Tackling transparency of beneficial ownership**

What are the issues identified by the Panama Papers?

The Panama Papers revealed that complex ownership structures have been used to hide links to criminal activities and tax obligations. They demonstrated the need for enhanced transparency on the ultimate beneficial ownership of certain legal entities needed to be further enhanced. The fourth AMLD already sets out a comprehensive framework as regards the collection, storing of, and access to information on the beneficial owners of companies, trusts and other corporate vehicles.

The Panama Papers highlighted areas where further enhancements would be advisable. The amendments put forward address these issues and will improve the transparency of beneficial ownership information by clarifying or strengthening some of its features: what is registered (i.e. entities for which information is registered), where registration must take place (which Member State is responsible for registration of a given entity), who is granted access to information (clearer access to information on beneficial ownership), how national registers should be interconnected. In addition, the Commission today announced separately [LINK TO TAX IP] that it would explore ways for information on beneficial ownership to be automatically exchanged between Member States' tax authorities.

Who will have access to the beneficial ownership information?

Currently, under the fourth AMLD, the information about the beneficial ownership of companies and trusts is already accessible to competent authorities and obliged entities in view of facilitating the performance of their "customer due diligence obligations" (i.e. a procedure consisting in properly identifying the customer on the basis of reliable and independent sources, such as for example identity cards or passports).

The Commission now proposes to also provide public access to certain essential beneficial ownership information held in registries regarding companies and trusts that engage in economic activities with a view to gain profit. For privacy reasons, access to information in relation to trusts not engaged in economic activities (e.g. family trusts set up to finance studies) will only be granted to persons and organisations that can demonstrate a legitimate interest.

Today's Communication on promoting tax transparency and fighting tax evasion also sets out our plans to make this information available to tax authorities, giving them all the information they need to crack down on those who do not pay their fair share of taxes.

What impact will the proposal have on the transposition of the Fourth AMLD by the Member States?

The formal transposition date for the fourth AMLD is 26 June 2017. 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 the Directive to Q4 2016.

Although Member States have sped up work, the period to transpose the fourth AMLD is still ongoing. Therefore we must carefully take into account the work already undertaken by the Member States when implementing and transposing rules that are closely linked to the issues that will be revised by the modifying Directive, such as for example the exemption regime for pre-paid cards.

In this respect, continuity must be ensured with the work already undertaken by the Member States regarding the creation of the registries/mechanisms mentioned in articles 30 and 31 of the Fourth Anti-Money Laundering Directive.

3. Protecting the EU financial system from high risk countries

Why does the Commission intend to adopt a list of high risk third countries?

The Fourth Anti-Money Laundering Directive mandates the Commission to identify "high-risk third countries" having strategic deficiencies in their regimes on Anti-Money Laundering (AML) and Countering Terrorist Financing (CFT). The purpose of this list is to protect the proper functioning of the EU financial system from the money laundering and terrorist financing risks emanating from those countries. This requirement follows the approach developed at global level by the Financial Action Task Force (FATF) to respond to the threat posed by countries that did not implement internationally agreed standards on AML/CFT.

In line with the risk-based approach, banks shall apply enhanced due diligence in case of financial flows to/from high risk third countries identified by the Commission.

Those enhanced measures will lead to extra checks and monitoring of those transactions by banks and obliged entities in order to prevent, detect and disrupt suspicious transactions. Hence these measures do not entail any type of sanctions, termination of business relationship, restrictions trade relations, or limiting our development assistance; it only aims to apply enhanced vigilance measures in those cases. The EU will continue to engage across all relevant policy areas with the concerned jurisdictions, including through development cooperation, the ultimate goal being their compliance and removal from the list.In order to further clarify the type of enhanced vigilance to be applied and avoid loopholes in the EU, the Commission proposes to harmonise those enhanced measures through a

revision of the Fourth Anti-Money Laundering Directive.

When will the list of high-risk third countries be applicable?

The Commission plans to adopt the Delegated Act identifying high-risk countries on 14 July 2016. According to the Fourth AMLD, the Delegated Regulation will then be transmitted to the European Parliament and Council who can express objections within a given period of time. The Delegated Regulation will enter into force if no objection has been expressed either by the European Parliament or the Council within a period of one month of the notification – which can be extended on request by one additional month (i.e. maximum 2 months in total) and the Delegated Regulation will be published in the Official Journal after this period and enters then into force.

For more information:

IP/16/2380

MEMO/16/2381

Press contacts:

Christian WIGAND (+32 2 296 22 53)
Melanie VOIN (+ 32 2 295 86 59)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email