EUROPEAN
COMMISSION

Brussels, 26.6.2017
SWD(2017) 241 final

PART 2/2

COMMISSION STAFF WORKING DOCUMENT

Accompanying the document

Report from the Commission to the European Parliament and to the Council

on the assessment of the risks of money laundeirng and terrorist financing affecting the internal market and relating to cross-border situations

{COM(2017) 340 final}

TABLE OF CONTENT

Annex 1 - RISK ANALYSIS BY PRODUCTS

Annex 2 – PROJECT CHARTER

Annex 3 - METHODOLOGY FOR THE SUPRANATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS

Annex 4 – OVERVIEW OF ENTITIES SUBJECT TO THE AML/CFT FRAMEWORK

Annex 5 – STATISTICS ON SUSPICIOUS TRANSACTION REPORTS

Annex 6 - EU LEGISLATION RELEVANT IN THE AML/CFT FIELD

Annex 7 - GLOSSARY

Annex 8 - BIBLIOGRAPHY

ANNEX 1 - RISK ANALYSIS BY PRODUCTS

The SNRA was carried out following a defined methodology allowing a systematic analysis of the ML or TF risks linked to modi operandi used by perpetrators. The aim was not to pass judgment on a sector as a whole, but to identify the circumstances according to which the services and products it delivers or provides could be abused for TF or ML purposes.

This SNRA is based on Directive 2005/60/EC (3AMLD) which was the legislation in force at the time of the analysis. It describes the areas in which, at the time, the EU legal framework was not as harmonised or complete as it would be once the forthcoming revisions of 3AMLD had taken effect. In particular, Directive (EU) 2015/849 (4AMLD) shall be transposed by 26 June 2017. Since the 4AMLD was not yet transposed at the time of the analysis, it was not considered as part of the legal framework in place for the risk analysis. The 4AMLD and its upcoming revision (COM(2016) 450) are, however, considered as part of the mitigating measures.

For each risk, a rating has been defined for the threat and vulnerability based on the criteria defined in the methodology (see annex 3). Those ratings are determined on a scale from 1 to 4 as follows:

1) Lowly significant (value: 1)
2) Moderately significant (value: 2)
3) Significant (value: 3)
4) Very significant (value: 4)

Those ratings were used only to synthesise the analysis. They should not be considered in isolation from the factual description of the risk.

Contents

Cash products 13
Cash couriers 14
Cash intensive business 20
High value banknotes 26
Payments in cash 30
Financial sector products 35
Retail financial sector – deposits on accounts 36
Institutional investment sector - Banking 40
Institutional investment sector - Brokers 43
Corporate banking sector 47
Private banking sector 51
Crowdfunding 55
Currency exchange 61
E-money sector 64
Transfers of funds 71
Illegal transfers of funds - Hawala 78
Payment services 82
Virtual currencies 90
Business loans 96
Consumer credit and low value loans 98
Mortgage credit and high value asset-backed credits 100
Life-Insurance 103
Non-Life Insurance 106
Safe custody services 109
Non-financial products 112
Creation legal entities and legal arrangements 113
Business activity of legal entities and legal arrangements 120
Termination of legal entities and legal arrangements 126
High value goods – artefacts and antiquities 131
High value assets – Precious metals and precious stones 136
High value assets – other than precious metals and stones 141

Couriers in precious metals and stones 144
Investment real estate 147
Services from accountants, auditors, tax advisors 150
Legal service from notaries and other independent legal professionals 155
Gambling sector products 160
General description of the gambling sector 161
Betting 163
Bingo 168
Casinos 171
Gaming machines (outside casinos) 176
Lotteries 180
Poker 184
Online gambling 187
Non-for-profit organisations 193
Collect and transfers of funds through a Non-Profit Organisation (NPO) 195
Horizontal vulnerabilities 201
Vulnerabilities linked to financial supervision 202
Vulnerabilities linked to Financial Intelligence Units 206

Cash products

Cash couriers

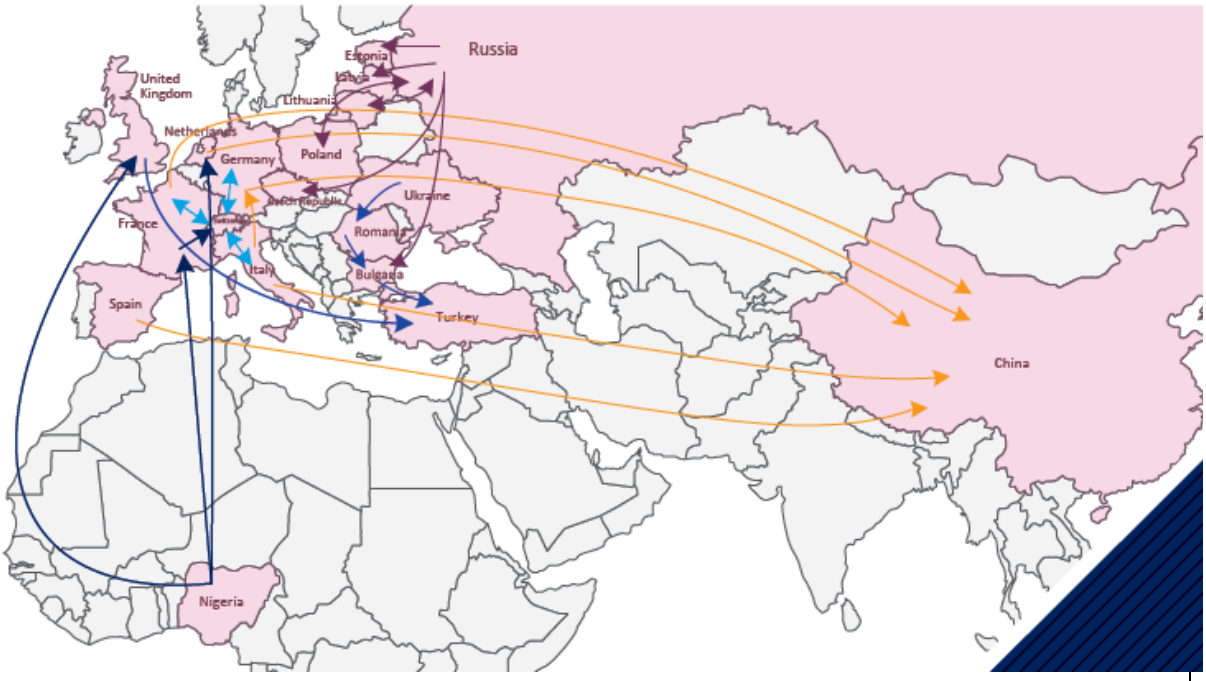
Product

Cash couriers / cross external border cash movements

General description of the sector and related product/activity concerned

This assessment covers the supranational risks – i.e. cash entering/leaving the European Union at the EU external borders.

Map of key countries of destination and origin for cash movements in and out of the EU



The Cash Control Regulation establishes a uniform EU approach towards cash controls based on a mandatory declaration system. If a natural person entering or leaving the EU (including transiting) transports cash of a value of EUR 10 000 or more, he/she must declare these funds. The EUR 10 000 threshold is considered high enough not to burden the majority of travellers and traders with disproportionate administrative formalities. However, when there are indications of illegal activities linked with movements of cash lower than EUR 10 000, the collecting and recording of information related to these movements is also authorised. This provision was introduced in order to limit the practice of 'smurfing' or 'structuring', the practice of deliberately carrying amounts lower than the threshold with the intention to escape the obligation to declare (e.g. splitting the amount between different connected persons from a same group/family).

The Cash Control Regulation is aimed at aligning EU legislation with the requirements of the FATF's Recommendation 32 on cash couriers and with the highest global AML/CFT standards. The definition of cash in the Cash Control Regulation matches the definition used by the FATF for Recommendation 32 on cash couriers and includes: ¬Currency, i.e. banknotes and coins that are in circulation as a medium of exchange. ¬Bearer-negotiable instruments (BNI)

As the Cash Control Regulation mirrors the definition of 'cash' used in the supra-national standard (FATF recommendation 32), gold, precious metals or stones, electronic cash cards and casino chips are currently not included in the definition of cash.

Statistics: On average, 100 000 cash control declarations are submitted annually in the EU, representing a total amount declared between 60-70 billion Euro. While amounts of undeclared or incorrectly declared cash which have been detected by authorities are highly variable (240 Mio – 1.5 billion Euro/year), on average approximately 300 Mio Euro per year is detected following controls. Statistics show a sustained, high level of cash declarations over the years and also a significant increase in the number of recordings at the EU border in recent years. It is difficult to pinpoint the exact combination of reasons behind these trends based on the available data.

General comment (where relevant)

This risk scenario is intrinsically linked to use of/payment in cash and to high value denomination banknotes risk scenario.

Criminals or terrorist financiers who generate/accumulate cash proceeds seek to aggregate and move these profits from their source, either to repatriate funds or to move them to locations where one has easier access to placement in the legal economy.

The characteristics of such locations are a predominant use of cash, more lax supervision of the financial system or stronger bank secrecy regulations. It may also be used by terrorists to transfer rapidly and safely funds from one location to another, including by using cash concealed in air transit.

Cash couriers may use air, sea or rail transport to cross an EU external border. In addition, cash may be moved across external borders unaccompanied such as in containerised or other forms of cargo, or concealed in mail or post parcels. If perpetrators wish to move very large amounts of cash, often a valuable option is to conceal it in cargo that can be containerised or otherwise transported across borders.

Perpetrators may also use sophisticated concealment methods of cash within goods which are either carried across the external border by a courier or are sent by regular mail or post parcel services. Although unaccompanied consignments tend to be smaller than those secreted within vehicles, or on the person of cash couriers, the use of high denomination banknotes can still result in seizures of significant value.

Threat

Terrorist financing

The assessment of the TF threat related to cash couriers/unaccompanied cash movements shows that terrorist groups have made use of various techniques to move physical cash across the external borders, particularly in the case of larger organisations.

This threat is particularly relevant for cash couriers from the EU to third countries. LEAs have seized large amounts of money in conflicts zones that was supposed to finance terrorist organisations. In addition, cases have been identified where (prospective) foreign terrorist fighters doubled as cash couriers to fund their travels and sojourn in conflict areas. These individuals typically carry lower amounts that are more difficult to detect and may not be subject to an obligation to declare incumbent on natural persons carrying EUR 10 000 Euro or more is cash. As it allows for anonymity, this modus operandi is perceived as attractive and fairly secure, despite still carrying some risks. That is the reason why this modus

operandi shall also be considered in conjunction with the analysis of high denomination banknotes. The more high denomination banknotes are used, the easier the cash transportation is – although risks associated with acquiring high denomination notes (not readily available) may not outweigh the benefit of additional compactness. Cash transportation is a recurring modus operandi for terrorist groups in Syria / ISIL occupied territories – although the average amounts carried by a foreign fighter leaving the EU may not be significant compared to locally available funds.

The threat of cash transportation into the EU from a third country may also exist, in particular from countries exposed to TF risks or conflict areas (e.g. cash couriers from Syria, Gulf region, Russia into the EU have been reported). There are limited indications of high-value movements of cash into the Union (i.e. much in excess of the declaration threshold) for the purposes of terrorism financing. Cases have been identified concerning lower amounts and involving integration of cash amounts carried from third countries into the financial system/legal economy of the EU (analysed in a separate fiche).

From a perpetrator risk-management perspective, sending cash through post or freight consignments, using multiple consignments each containing lower amounts presents a theoretically attractive option as there is no courier physically crossing the external border carrying the cash who could be intercepted. While customs controls may take place, these do not allow for the capture of all relevant data.

Finally, perpetrators may also have an incentive to convert cash in other types of anonymous assets which are not subject to cash declarations (gold, prepaid cards - covered by separate fiche).

Conclusions: LEAs have gathered evidence that cash couriers are recurrently used by terrorist groups to finance their activities or fund FTF travels. Similarly to the analysis conducted on cash, the use by criminal elements or terrorist financiers of cash couriers present advantages since this modi operandi is easily accessible, with no specific planning or expertise required. In that context, the level of TF threat related to cash couriers is considered as very significant (level 4).

Money laundering

The assessment of the ML threat related to cash couriers presents some commonalities with TF threats. Organised crime organisations also recurrently make use of cash couriers for the same reasons: easily accessible, no expertise, no planning and low cost. This modus operandi is very attractive for organised crime since it offers an alternative vs. the use of the formal financial sector to move funds while allowing full anonymity. Numerous cases of suspicious cash transports have been reported by law enforcement authorities (either in connection with predicate offenses to money-laundering such as drug trafficking and other serious crimes or as separate incidents).

Similarly cases were reported for other types of cash-like instruments (gold, anonymous prepaid cards), which are outside the scope of this fiche (see separate fiches).

Since specific controls are focusing on physical transportation by natural persons, perpetrators may find sending cash by post/freight/shipping more attractive and more secure. There is anecdotal evidence that this modus operandi was used but the size of the problem is difficult to quantify (see IA on CCR revision).

Conclusions: the level of ML threat related to cash couriers is considered as very significant (level 4)

Vulnerability

Terrorism Financing

(a) risk exposure:
The assessment of the TF vulnerability related to cash couriers shows that due to the nature of cash, the use of cash couriers allows significant volumes of transactions/transportation to take place speedily and anonymously.
The cross-border aspect of this modus operandi increases the risk to involve geographical areas identified as high risks.

(b) risk awareness:
The legislation in place (mandatory cash declarations by natural persons at the external borders of the EU) has increased the risk awareness, at least as far as persons are concerned. Risk awareness exists for unaccompanied cash transportation – but is more limited.

(c) legal framework and controls:
There are controls in place through the mandatory declaration of cash transportation at the EU external borders (Cash Control Regulation). This legislation has increased the risk awareness, at least as far as natural persons are concerned. These cash declarations allow for easier detection of suspicious transactions and reporting to the FIUs (although shortcomings in information sharing exist).

Where unaccompanied cash is concerned (cash sent through consignments or parcels) the present legal framework relies mainly on customs controls, which do not allow the capture of all relevant data.

Conclusions: The risk exposure related to cash couriers by physical persons is intrinsically linked to the cash based activity (large volume, anonymity, speediness) - which is exacerbated by the fact that –especially within a terrorism context- the individual couriers often carry amounts below the declarative threshold. While the volume of cash couriers may be more important than for unaccompanied shipping, risk awareness and controls are in place.
The use of cash couriers or methods to ship in/out of the EU unaccompanied cash coupled with the anonymity of cash and (at least with respect to unaccompanied cash) an imperfect control mechanism presents a significant challenge. While the volume of unaccompanied cash shipped in/out the EU is probably lower than for accompanied cash couriers, the risk awareness and controls of the latter pose a greater challenge.
In that context, the level of TF vulnerability related to cash couriers by natural persons is considered as significant (level 3). The level of TF vulnerability related to post/freight is considered as very significant considering the controls/legal framework in place, more than the inherent risk exposure (level 4).

Money Laundering

(a) risk exposure
The assessment of the ML vulnerability related to cash couriers shows that the risk exposure is intrinsically linked to the cash based activity (anonymity, speediness). Hence the risk exposure is particularly important for this modus operandi.

(b) risk awareness

The legislation in place (mandatory cash declarations at the external borders for cash carried by natural persons) has increased the risk awareness, at least as far as persons are concerned.

Risk awareness exists for unaccompanied physical cash transportation – but is more limited with regard to shipping/freight/couriers.

(c) legal framework and controls

Similarly to TF, there are controls in place through the mandatory declaration of cash transportation at the EU external borders (Cash Control Regulation) by natural persons.

These cash declarations allow an easier detection of suspicious transactions and are reported to the FIUs (although shortcomings in information sharing exist and enforcement in application may also vary between Member States).

Where unaccompanied cash is concerned (cash sent through consignments or parcels) the present legal framework relies mainly on customs controls, which do not allow the capture of all relevant data.

Conclusions: The risk exposure related to cash couriers by physical persons is intrinsically linked to the cash based activity (large volume, anonymity, speediness). While the volume of cash couriers may be more important, the risk awareness and the controls in place exist. The use of cash couriers or methods to ship in/out of the EU unaccompanied cash coupled with the anonymity of cash and (at least with respect to unaccompanied cash) an imperfect control mechanism presents a significant challenge. While the volume of unaccompanied cash shipped in/out the EU is probably lower than for accompanied cash couriers, the risk awareness and controls in place pose a greater challenge. In that context, the level of ML vulnerability related to cash couriers by natural persons is considered as significant (level 3) and by post/freight is considered as very significant (level 4).

Mitigating measures

The Commission will present a legislative proposal revising the cash control Regulation to further mitigate those risks. In order to provide competent authorities with adequate tools, the proposal intends to:

- Enable authorities to act on amounts lower than the declaration threshold of EUR10 000, where there are suspicions of criminal activity,
- Improve the exchange of information between authorities and Member States;
- Enable competent authorities to demand disclosure for cash sent in unaccompanied consignments such as cash sent in postal parcels or freight shipments;
- Extend the definition of 'cash' to also include precious commodities acting as highly liquid stores of value such as gold, and to prepaid payment cards which are currently not covered by the standard cash control declaration.

Cash intensive business

Product

Cash intensive business

Sector

sectors of bars, restaurants, constructions companies, motor vehicle retailers, car washes, art and antique dealers, auction houses, pawnshops, jewelleries, textile retail, liquor and tobacco stores, retail/night shops, gambling services

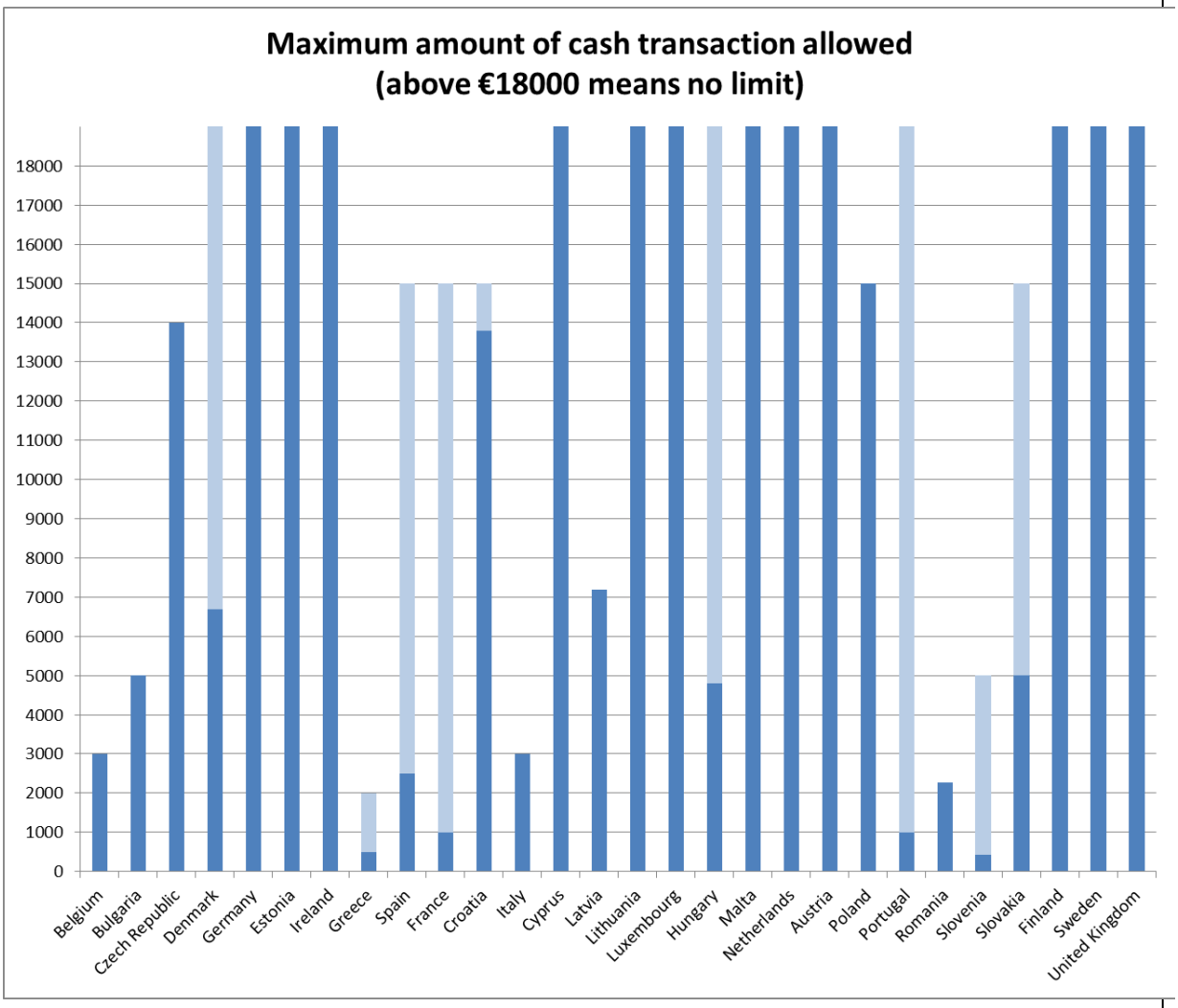
General description of the sector and related product/activity concerned

An interesting description of the use of cash has been described by the European Central Bank in its report *Consumer cash usage. A cross-country comparison with payment diary survey data* (ECB Working Paper Series, no 1685, 2014) <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf>

Concerning cash limitations, 12 Member States (Germany, Estonia, Ireland, Cyprus, Lithuania, Luxembourg, Malta, Netherlands, Austria, Finland, Sweden, United Kingdom) do not have any restrictions on cash payments. In most countries, large value cash payments triggered obligations under the anti-money laundering provisions of the Directive or national legislation – along the following lines:

Country	Limitation	Scope
Belgium	EUR 3 000 (and 10% of any transaction above EUR 3 000)	All persons acting as business
Bulgaria	BGN 10000 (EUR 5 000)	All persons and transactions except bank operations and salaries
Czech Republic	CZK 270 000 (EUR 14 000)	All persons and transactions
Denmark	DKK 50 000 (EUR 6 700)	Businesses not covered by AML Act
Greece	EUR 1 500 for business to consumer, EUR 500 for business to business,	All persons acting as business
Spain	EUR 2 500 EUR 15 000 for non-residents natural persons	All persons acting as business
France	EUR 1000 EUR 15 000 for non-residents	All persons acting as business
Croatia	HRK 105 000 (EUR 13800), EUR 15 000 for non-residents	All persons acting as business
Italy	EUR 3 000	All persons and transactions
Latvia	EUR 7 200	All persons acting as business
Hungary	HUF 500 000 (EUR 4 800)	Business to business transactions

Country	Limitation	Scope
Poland	EUR 15 000	All persons acting as business
Portugal	EUR 1 000	Legal persons
Romania		
Slovenia	EUR 420 for payments EUR 5 000 for receiving	All persons acting as business
Slovakia	EUR 5 000 for businesses, EUR 15 000 for natural persons	All persons and transactions, with different limits



(the previous chart ignores the absence of restriction for non-business transactions between private persons)

The following general observations can be made:

- Limitations typically apply to transactions in both national and foreign currencies, the limit being in such case the equivalent of the national limit in that currency.
- Limitations apply to single payments exceeding the thresholds, but legislations often consider that multiple payments connected to a single operation should be considered as

one.

- Limitations always concern at least businesses and transactions between businesses and customers. Non-business transactions between natural persons are often not concerned by the limitation (BE, DK, GR, ES, FR, HR, LV, HU, PL, PT).
- Limitations typically apply to transactions in cash (i.e. banknotes). Some national legislations extend explicitly the limitations to bearer instruments (ES, IT)

Description of the risk scenario

Cash intensive business is used by perpetrators:

- to launder large amounts of cash, which are proceeds of criminal activity, by claiming that the funds originate from economic activities;

- to launder amounts of cash, which are proceeds of criminal activity, by justifying its origin based on fictitious economic activities (both for goods and services)

- to finance, through often small amounts of cash, terrorist activities without any traceability

General comment (where relevant)

This risk scenario is intrinsically linked to use of/payment in cash and to high value denomination banknotes risk scenario.

Threat

Terrorist financing

The assessment of the TF threat related to cash intensive business shows that cash intensive businesses are generally run by individuals through bars, restaurants, phone shops but are managed by a network of persons forming a terrorist organisation. In general, they are used to get clean cash in a speedy way (e.g. selling cars or jewelleries). However, this risk scenario is not used equally by all terrorist organisations (never seen for Daesh for instance) and not largely widespread as it requires capabilities to run the business.

Conclusions: the elements gathered by the LEAs and FIUs show only few cases have been registered meaning that terrorist groups do not favour this risk scenario as it requires some technical expertise and investments to run the business in itself which makes this modus operandi less attractive. However, since this risk is not only hypothetical and that sleeper cells are active in cash intensive businesses, the level of TF threat related to cash intensive business is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to cash intensive business shows that this modus operandi is exploited by criminals as it represents a viable option which is rather attractive and secure. It constitutes the easiest way to hide illegitimate proceeds of crime. However, as for TF, it requires a moderate level of expertise to be able to run the business and to escape detection.

Conclusions: cash intensive businesses are favoured by criminal organisations to launder proceeds of crime. As it requires some level of expertise to run the business, the level of ML threat related to cash intensive business is considered as significant (level 3).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to cash intensive business shows that the main factors are linked to the risk posed by cash.

(a) risk exposure

While cash intensive business is less attractive to terrorist organisations than to criminals (see threat assessment below), when they are used by terrorists they present some vulnerabilities because the underlying risk is the one related to cash. The vulnerability assessment of TF related to cash intensive business is intrinsically linked to the assessment related to the use of/payments in cash in general and can follow the same rationale. Cash intensive businesses allow the processing of a huge number of anonymous transactions which require no management of new technologies and tracking tools. Hence it has a high inherent risk exposure.

(b) risk awareness

The risk awareness appears to be quite low because, even if large sums of cash can be obtained from cash intensive business, some FIUs notice that terrorist organisations seem to prefer lower denomination banknotes which are less easy to be considered as suspicious by obliged entities and LEAs.

(c) legal framework and controls in place

The legal frameworks in place related to cash payment limitations that some Member States have introduced. This framework varies a lot from one Member State to another concerning cash controls and cash payment limitations and, thus, controls can potentially be inexistent.

Conclusions: the vulnerability of cash intensive business is intrinsically linked to the vulnerabilities related to the use of cash in general. The variety of legal frameworks in place, the widespread use of cash in EU economies and the fact that the sector seems being not aware of this risk, the level of TF vulnerability related to cash intensive business is considered as very significant (level 4).

Money laundering

The assessment of the ML vulnerability related to cash intensive business shows that the main factors are linked to the risk posed by cash.

(a) risk exposure

The vulnerability assessment of ML related to cash intensive business is intrinsically linked to the assessment related to the use of/payments in cash in general and can follow the same rational. Cash intensive businesses allow the processing of a huge number of anonymous transactions which require no management of new technologies and tracking tools. This risk exposure concerns cash payments both for goods and services. Hence it has a high inherent risk exposure.

(b) risk awareness

Obliged entities are usually aware about the risk posed by cash – although controls are not easy to implement. However, for other professions not submitted to AML/CFT obligations, risk awareness remains a challenge.

(c) legal framework and controls in place

There is no uniform level of controls at EU level, for instance through common rules on cash

limitations or cash transactions reports.

The vulnerability of the sector is affected by the existence, or lack thereof, of rules relating to cash payment limitations:

- where cash limitation rules exist, ML vulnerabilities related to cash intensive business have been more easily mitigated thanks to the legal requirements which allow the refusal of cash payments above a certain threshold. In these cases, controls are in place and allow detecting red flags and suspicious transactions more easily. In addition, these cash payment thresholds are perceived by the sector and by LEAs as more efficient and, eventually, less burdensome than imposing customer due diligence measures. However, these legal businesses can also hide shadow and illicit activities which are able to circumvent the cash limitations.

- where cash limitations rules do not exist, and whilst the risk awareness is quite high, the sector does not know how to manage the risks. It has no tools to control and detect suspicions transactions. The result is that the number of STRs is rather low, or even inexistent.

Some Member States have introduced cash transaction reports to be declared for cash operations over a certain threshold. However, there is no common approach at EU level.

From an internal market perspective, the differences between Member States legislations on cash limitations increases the vulnerability for the internal market; perpetrators may more easily circumvent controls in their country of origin by investing in cash intensive business in another Member States having lower/no control on cash limitation. The existence of cash payments limitations in some Member States, and their absence in other Member States, creates the possibility to bypass the restrictions by moving to the Member States where there are no restrictions, whilst still conducting their terrorist or other illegal activities in the 'stricter' Member State.

The 3rd AML Directive provides that high value dealers accepting payment in cash beyond EUR 15 000 are subject to AML/CFT rules and have to apply CDD requirements. This obligation applies to any persons trading in goods when the payment is made in cash beyond EUR 15 000 – but it does not cover services. However, the effectiveness of those measures is still limited given the number of STRs. The volume of STR reporting is generally low because cash transactions are difficult to detect, there is not much available information and dealers may lose their clients to the benefit of competitors applying looser controls. In addition, it may be difficult for a trader in high value goods to design an AML/CFT policy in the limited events where a cash transaction beyond the threshold takes place (i.e. it is not the sector in itself which is covered by AML/CFT regime – but only high value dealers faced with cash transactions beyond a threshold). For this reason, some Member States have extended the scope to cover certain sectors regardless of the use of cash. Some Member States have also decided to apply a general cash restriction regime at this threshold to reduce the risk of ineffective or cumbersome application of CDD rules by high value dealers. However, it does not mitigate situations of cash intensive business which are based on lower amount cash transactions – or a repeated number of low amount cash transactions.

In addition, cash intensive businesses are inherently risky because there are no rules dealing with fit and proper testing of these businesses' managers. Some cash intensive businesses are more vulnerable than others because they may give rise to cash exchange more easily (motor retails or pawnshops).

Conclusions: the risk exposure to ML of cash intensive businesses is influenced by the existence of legal cash limitations which are efficient to mitigate the risks but are not always sufficient. In a cross-border context, the variety of regulations on cash payments constitutes also a factor of vulnerabilities. When no rules are in place, the risk awareness of the sector is quite low, leading to few STRs to FIUs. Investigative capacities from LEAs are then quite limited. In light of this, the level of ML vulnerabilities related to cash intensive businesses is considered as very significant (level 4).

Mitigating measures

- The Commission examines launching an initiative to swiftly reinforce the EU framework on the prevention of terrorism financing by enhancing transparency of cash payments through an introduction of a restriction of cash payments or by any other appropriate means. Organised crime and terrorism financing rely on cash for payments for carrying out their illegal activities and benefitting from them. By restricting the possibilities to use cash, the proposal would contribute to disrupt the financing of terrorism, as the need to use non anonymous means of payment would either deter the activity or contribute to its easier detection and investigation. Any such proposal would also aim at harmonising restrictions across the Union, thus creating a level playing field for businesses and removing distortions of competition in the internal market. It would additionally foster the fight against money laundering, tax fraud and organised crime.

- The Commission will continue to monitor the application of AML/CFT obligations by dealers in goods covered by the AMLD and further assess risks posed by providers of services accepting cash payments. It will further assess the added value and benefit for making additional sectors subject to AML/CFT rules.

- Member States should take into account in their national risk assessments the risks posed by payment in cash in order to define appropriate mitigating measures such as the introduction of cash limits for payments, Cash Transaction Reporting systems, or any other measures suitable to address the risk. Member States should consider making sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of their NRA.

High value banknotes

Product

High value banknotes

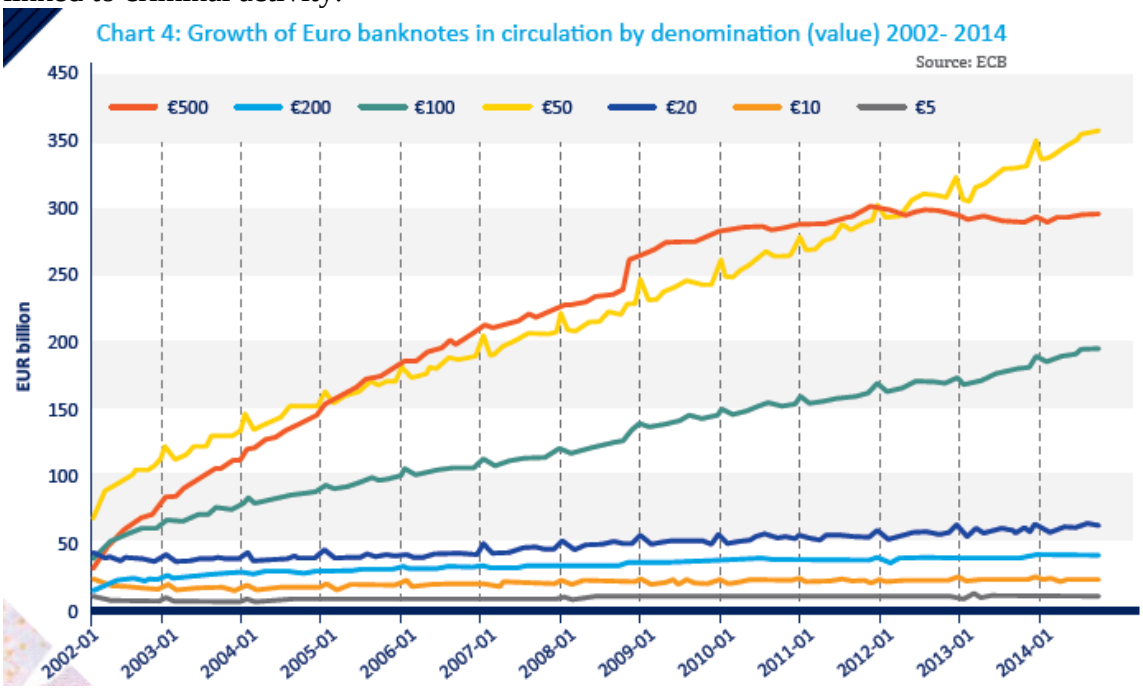
Sector

/

General description of the sector and related product/activity concerned

In spite of steady growth in non-cash payment methods and a moderate decline in the use of cash for payments, the total value of euro banknotes in circulation continues to rise year-on-year beyond the rate of inflation. Cash is largely used for low value payments and its use for transaction purposes is estimated to account for around one-third of banknotes in circulation. Meanwhile the demand for high denomination notes, such as the EUR 500 note, not commonly associated with payments, has been sustained. These are anomalies which may be linked to criminal activity.

Chart 4: Growth of Euro banknotes in circulation by denomination (value) 2002- 2014



Perhaps the most significant finding around cash is that there is insufficient information around its use, both for legitimate and illicit purposes. The nature of cash and the nature of criminal finances mean that there is little, if any, reliable data available on the scale and use of cash by ordinary citizens, let alone by criminals.

One of the few reliable figures available, that of the volume and value of bank notes issued and in circulation in the EU, leaves open questions around the use to which a large proportion of cash in issuance is put, especially when considering the EUR 500 note. From a total of approximately EUR 1 trillion banknotes in circulation as of end-2014, the use of a significant proportion of these remains unknown. Furthermore, the EUR 500 note alone accounts for over 30% of the value of all banknotes in circulation, despite it not being a common means of payment. Although it has been suggested that these notes are used for

hoarding, this assumption is not proven. Even if this is the case, the nature of the cash being hoarded (criminal or legitimate) is unknown.

Description of the risk scenario

Perpetrators use high value denominations, such as EUR 500 banknotes, to make the cash transportation easier (the larger the denomination, the more funds can be shrunk to take up less space).

General comment (if relevant)

This risk scenario is intrinsically linked to use of/payment in cash and to cash intensive business risk scenario

Threat

Terrorist financing

The assessment of the TF threat related to high value denomination banknotes shows that terrorist groups are not really keen in using high value denominations. They are not necessarily easy to access and, given that they can be detected quite easily they are not attractive for terrorist groups whose first objective is to get cash as quickly as possible. For sake of discretion, terrorist groups tend to favour low denominations banknotes. LEAs have detected few cases which tend to demonstrate that the intent and capability are not really significant.

Conclusions: in that context, the level of TF threat related to high value denominations banknotes is considered as moderately significant (level 2)

Money laundering

The assessment of the ML threat related to high value denomination banknotes shows that they are recurrently exploited by criminal organisations to launder proceed of crime. The risk related to high value banknotes is not limited to EUR 500 and as long as long large sums in cash are gathered they are considered as attractive by criminal organisations. It does not require any major planning or complex operation – i.e. perpetrators have the technical skills to easily use this product. It remains a "low cost" operation and allows storing of large amounts in very small volumes – which makes it very attractive for organised crime. It has been reported by LEAs that some criminal groups seek EUR 500 banknotes by paying a premium in order to get access to those large denominations; this demonstrates its attractiveness.

Conclusions: banknotes (EUR 500 but not only) are used recurrently by criminal organisations. This modus operandi is widely accessible and available at low cost. For ML purposes, it's quite easy to abuse and requires no specific planning or knowledge. In that context, the level of ML threat related to high value denomination banknotes is considered as very significant (level 4)

Vulnerability

Terrorist financing

The assessment of TF vulnerability related to high value denomination banknotes shows that this product is as vulnerable for TF as for ML for the following reasons:

(a) risk exposure
Large volume of high value denominations is in circulation, despite low use in commercial transactions. Cash still allows carrying transactions in an expedited, anonymous, and untraceable way.

(b) risk awareness
Especially LEAs and FIUs have high risk awareness, as do obliged entities subject to AML/CFT obligations. Risk awareness of sectors not covered by AML/CFT obligations or cash limitations obligations remains challenging. Existing literature, especially Europol reports, point to the blind spot in risk awareness (i.e. the precise use of high value denominations, difference of issuance between Member States, disconnection with GDP). There is little, if any, reliable data available on the scale and use of cash by ordinary citizens, let alone by criminals.

(c) legal framework and controls in place
Even if terrorist groups are less attracted to high value denomination banknotes, detection is quite difficult because there is no EU harmonisation concerning the legal framework related to the use of high value denomination banknotes. Controls are uneven; reports to FIUs are rather few, and most of the time they cannot distinguish between ML and TF. The use of high value denomination banknotes for ML purposes may be impacted by the ECB decision to gradually phase out EUR 500 (may 2016) because of the recognised links with criminal activities. However, the return rate is generally quite low and these banknotes may be still in use for a long time. Therefore, this cannot be seen as an immediate mitigation measure.

Conclusions: from a vulnerability point of view, risk exposure is high, level of awareness is low and controls in place are not harmonised which create potential loopholes when cross-border transactions are at stake. In light of this, the level of TF vulnerability related to high value denomination banknotes is considered as very significant (level 4).

Money laundering

The assessment of ML vulnerability related to high value denomination banknotes shows the following features:

(a) risk exposure
High value denominations allow the storing/putting into circulation of large volumes of cash in a speedy and anonymous way. A large volume of high value denominations is in circulation, despite the low level of use in commercial transactions. Even if the use of high value denominations raises red flags, it remains that these denominations are not necessarily used for payments but rather to move funds. Large amounts can be stored in very small volumes. They are less easy to detect by FIUs and obliged entities.

(b) risk awareness
Especially LEAs and FIUs have high risk awareness, as do obliged entities subject to AML/CFT obligations. Risk awareness of sectors not covered by AML/CFT obligations or cash limitations obligations remains challenging. Existing literature, especially Europol reports, point to the blind spot in risk awareness (i.e. the precise use of high value denominations, difference of issuance between Member States, disconnection with GDP). There is little, if any, reliable data available on the scale and use of cash by ordinary citizens,

let alone by criminals.

(c) legal framework and controls in place

The use of high value denomination banknotes for ML purposes may be impacted by the ECB decision to gradually phase out EUR 500 (May 2016) because of the recognised links with criminal activities. The issuance of the EUR 500 will be stopped around the end of 2018. However, the return rate is generally quite low and these banknotes may be still in use for a long time. The EUR 500 will remain legal tender and can therefore continue to be used as a means of payment and store of value. Therefore, this cannot be seen as an immediate mitigation measure.

<u>Conclusions:</u> similarly to the outcomes of the assessment of the TF vulnerability related to high value denomination banknotes, the ML vulnerability related to these products is considered as <u>very significant</u> (level 4).

Mitigating measures

- Monitoring of the return rate of EUR 500 banknotes will be conducted as well as an assessment of the evolution of the usage of the EUR 200 banknote.

Payments in cash

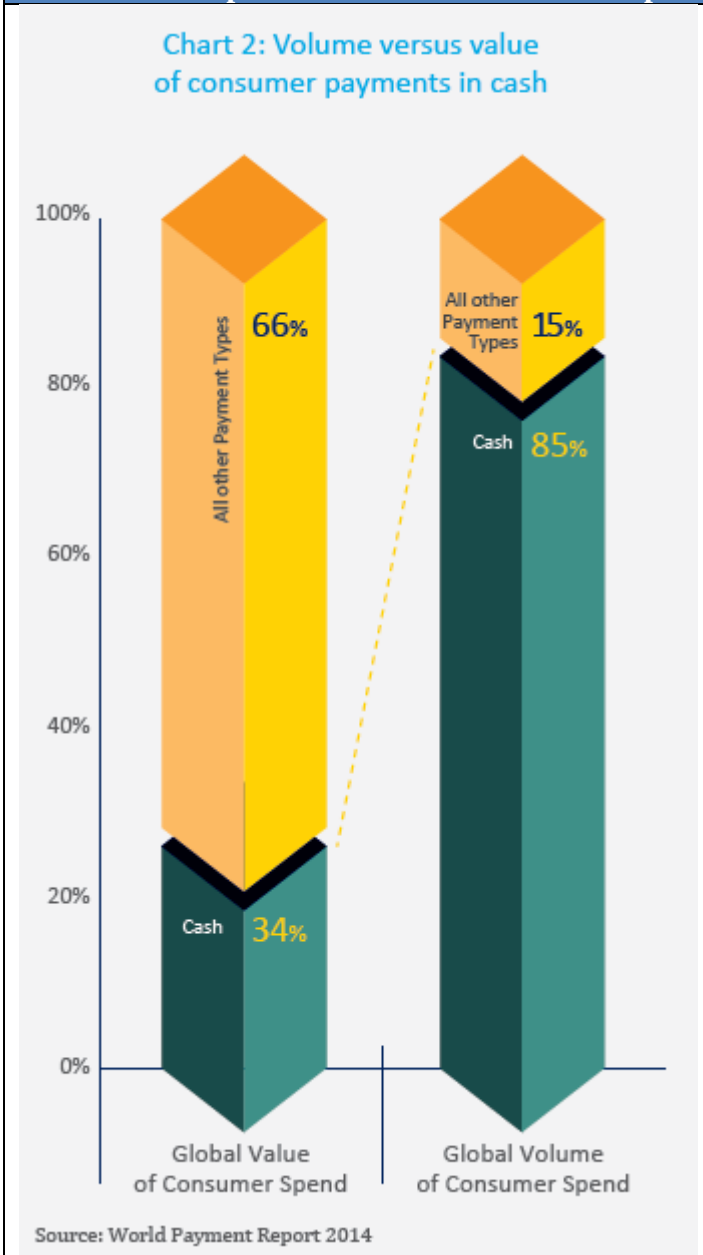
Product

Payments in cash

Sector

/

General description of the sector and related product/activity concerned



Certain studies suggest that cash transactions have been moderately declining at a rate of between 1.3 – 3.3% per year7. This appears to correspond with available information around the growth of non-cash payment methods (an increase of about 4.2% for Europe8) and information on EU citizens' access to banking services (around 89% of adults have bank accounts compared to just 41% in the developing world)9. However payments in cash are still widespread; according to ECB data, 87% of all transactions below EUR 20 are still made in cash.

7 http://www.richmondfed.org/publications/research/working_papers/2014/pdf/wp14-09.pdf

8 http://www.ecb.europa.eu/press/pr/date/2013/html/pr130910.en.html

9 http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-6025

Description of the risk scenario

Perpetrators frequently need to use a significant portion of the cash that they have acquired to pay for the illicit goods they have sold, to purchase further consignments, or to pay the various expenses incurred in transporting the merchandise to where it is required. Despite the advantages and disadvantages of dealing in cash (detailed earlier in this report) for criminal

groups, there is often little choice. The criminal economy is still overwhelmingly cash based. This means that, whether they like it or not, perpetrators selling some form of illicit product are likely to be paid in cash. The more successful the perpetrators are and the more of the commodity they sell, the more cash they will generate. This can cause perpetrators significant problems in using, storing and disposing of their proceeds. Yet despite these problems, cash is perceived to confer some significant benefits on them.

In addition, the objective of criminals is to launder large amounts of cash, which are proceeds of criminal activity, by claiming that the funds originate from economic activities. They may launder amounts of cash, which are proceeds of criminal activity, by justifying its origin based on fictitious economic activities (both for goods and services). Terrorists may finance, through often small amounts of cash, terrorist activities without any traceability (see general description under cash intensive business).

General comment (where relevant)

This risk scenario is intrinsically linked to cash intensive business and high value denomination banknotes risk scenario.

Threat

Terrorist financing

The assessment of the TF threat related to payments in cash shows that terrorist groups use recurrently cash, as this modus operandi is widely accessible and low cost. Cash is at the basis of all illicit trafficking and illicit purchase of products. In general, cash is really attractive, difficult (even impossible) to detect and does not require specific expertise to be used.

Conclusions: based on the feedback from LEA and FIUs, the level of TF threat is considered as very significant (level 4).

Money laundering

The assessment of the ML threat related to payments in cash is considered as similar to the assessment of TF threat. For ML, cash is also the preferred option for criminals, which allows hiding illicit proceeds of crime easily and moving funds rapidly, including cross-border. As for TF, it does not require specific expertise, knowledge or planning capacities.

Conclusions: based on the feedback from LEA and FIUs, the level of ML threat is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of TF vulnerability related to payments in cash shows the following features:

(a) risk exposure
Cash payments allow speedy and anonymous transactions. The level of risk exposure is very high considering that large sums can also be moved across borders and may involve high risk customers and/or geographical areas.

(b) risk awareness
Especially LEAs and FIUs have high risk awareness, and so do obliged entities subject to AML/CFT obligations. Risk awareness of sectors not covered by AML/CFT obligations or

cash limitations obligations remains challenging. Existing literature, especially a Europol report, points to the blind spot in risk awareness (i.e. the precise use of high value denominations, difference of issuance between Member States, disconnection with GDP). There is little, if any, reliable data available on the scale and use of cash by ordinary citizens, let alone by criminals.

(c) legal framework and controls in place

While cash payment limitations may allow a mitigation of the level of vulnerability, legal frameworks in place related to cash payment limitations vary a lot from one Member State to another and, therefore, controls can potentially be inexistent. From an internal market perspective, the differences between Member States legislations on cash limitations increases the vulnerability for the internal market; perpetrators may more easily circumvent controls in their country of origin by investing cash intensive business in another Member States having lower/no control on cash limitation.

The 3rd AML Directive provides that high value dealers accepting payment in cash beyond EUR 15 000 are subject to AML/CFT rules and have to apply CDD requirements. This obligation applies to any persons trading in goods when the payment is made in cash beyond EUR 15 000 – but it does not cover services. However, the effectiveness of those measures is still limited considering the number of STRs. The volume of STR reporting is generally low because cash transactions are difficult to detect, there are few available information and dealers may lose their clients for the benefit of competitors applying looser controls. For those Member States who have put in place CTR, most of the time they are not connected to any STR and the analysis cannot be conducted (for instance, large sums withdrawn from an ATM will trigger CTR but no specific suspicion is related to that and the FIU cannot launch any investigation).

In addition, it may be difficult for a trader in high value goods to design an AML/CFT policy in the limited events where a cash transaction beyond the threshold takes place (i.e. it is not the sector in itself which is covered by AML/CFT regime – but only high value dealers faced with cash transactions beyond a threshold). For this reason, some Member States have extended the scope to cover certain sectors regardless of the use of cash. Some Member States have also decided to apply a general cash restriction regime at this threshold to reduce the risk of ineffective or cumbersome application of CDD rules by high value dealers. However, it does not mitigate situations of cash intensive business which are based on lower amount cash transactions – or a repeated number of low amount cash transactions.
In any case, some competent authorities consider that even when cash payment limitations exist, enforcement of these limitations is very challenging and may limit their impact on TF activities.

<u>Conclusions</u>: considering that cash payments may engage large transactions speedily and anonymously, including cross-border, that all sectors may potentially be exposed to cash payments and even if they are aware that these payments present some risks are not equipped to mitigate them (either because no framework/controls in place, or because enforcement of the controls is not efficient), the level of TF vulnerability related to payments in cash is considered as <u>very significant (level 4).</u>

<u>Money laundering</u>

The assessment of ML vulnerability related to payments in cash shows the following

features:

(a) risk exposure
The sector shows the same vulnerability to TF as to ML. As for TF, cash payments allow speedy and anonymous transactions to launder proceeds of ML crime. The level of risk exposure is very high considering that large sums can also be moved across borders and may involve high risk customers and/or geographical areas.

(b) risk awareness
Especially LEAs and FIUs have high risk awareness, and so do obliged entities subject to AML/CFT obligations. Risk awareness of sectors not covered by AML/CFT obligations or cash limitations obligations remains challenging. Existing literature, especially the Europol report, points to the blind spot in risk awareness (i.e. the precise use of high value denominations, difference of issuance between Member States, disconnection with GDP). There is little, if any, reliable data available on the scale and use of cash by ordinary citizens, let alone by criminals.

(c) legal framework and controls in place
While cash payment limitations may allow mitigating the level of vulnerability, legal frameworks in place related to cash payment limitations vary a lot from one Member State to another and, therefore, controls can potentially be inexistent. From an internal market perspective, the differences of Member States legislation in cash limitations increases the vulnerability for the internal market; perpetrators may more easily circumvent controls in their country of origin by investing cash intensive business in another Member States having lower/no control on cash limitation.
The volume of reporting is very low because cash transactions are difficult to detect. For those Member States who have put in place CTR, most of the time they are not connected to any STR and the analysis cannot be conducted (for instance, large sums withdrawn from an ATM will trigger CTR but no specific suspicion is related to that and the FIU cannot trigger any investigation).
In any case, some competent authorities consider that even when cash payment limitations exist, enforcement of these limitations is really challenging and may limit their impact on ML activities.

Conclusions: considering that cash payments may engage large transactions speedily and anonymously, including across border, that all sectors may potentially be exposed to cash payments and even if they are aware that these payments present some risks are not equipped to mitigate them (either because no framework/controls in place, or because enforcement of the controls is not efficient), the level of ML vulnerability related to payments in cash is considered as very significant (level 4).

Mitigating measures

- The Commission examines launching an initiative to swiftly reinforce the EU framework on the prevention of terrorism financing by enhancing transparency of cash payments through an introduction of a restriction of cash payments or by any other appropriate means. Organised crime and terrorism financing rely on cash payments for carrying out their illegal activities and benefitting from them. By restricting the possibilities to use cash, the proposal would contribute to disrupt the financing of terrorism, as the need to use non anonymous means of payment would

either deter the activity or contribute to its easier detection and investigation. Any such proposal would also aim at harmonising restrictions across the Union, thus creating a level playing field for businesses and removing distortions of competition in the internal market. It would additionally foster the fight against money laundering, tax fraud and organised crime.

- The Commission will continue to monitor the application of AML/CFT obligations by dealers in goods covered by the AMLD and further assess risks posed by providers of services accepting cash payments. It will further assess the added value and benefit for making additional sectors subject to AML/CFT rules.

- Member States should take into account in their national risk assessments the risks posed by payment in cash in order to define appropriate mitigating measures such as the introduction of cash limits for payments, Cash Transaction Reporting systems, or any other measures suitable to address the risk. Member States should consider making sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of their NRA.

Financial sector products

Retail financial sector – deposits on accounts

Product
Deposits on accounts
Sector
Credit and financial institutions
General description of the sector and related product/activity concerned
As far as trends are concerned, according to data from the European Banking Federation[1] since 1998, the total stock of deposits in the EU contracted slightly, by 2.4% in 2013, but returned to a pattern of growth in 2014 (+0.2%). While the contraction in 2013 was generated in the euro area, the rise from 2014 onwards is only attributable to the euro area countries where bank deposits expanded by EUR171.3 billion or 1.0%. At the same time, non-euro area EU countries' deposits contracted by EUR127.9 billion or 2.4%. In total, the 76.7% of all EU deposits are held by banks headquartered in the euro area. This share has changed very marginally in the last few years.
Description of the risk scenario
Perpetrators place the proceeds of crime into the financial system through the regulated credit and financial sector in order to hide its illegitimate origin. Terrorists, supporters or facilitators place funds from legitimate sources into the financial system with a view of using it for terrorist purposes. Money mules mechanisms may be used to transfer proceeds out of the banking sector using personal accounts either through cybercrime (scamming, fake banking websites etc.), money value transfer services.
Threat
Terrorist financing The assessment of the TF threat related to deposits on account /retail banking shows that this risk scenario concerns both placing funds and withdrawing funds (i.e. deposits on account and use of this account). It is frequently used by terrorists but also by relatives/friends and this extends the scope of the intent and capability analysis. Furthermore, law enforcement authorities have reported the use of forged or stolen documents by terrorists to open bank accounts. According to information from competent authorities, foreign terrorist fighters are generally withdrawing bank accounts' deposits through ATMs located in high risk third countries or conflict zones in general or in bordering countries. Terrorists outside conflict zones also withdraw funds through ATMs in order to pay in cash some of the expenses related to their operations. The source of the funds deposited on bank accounts may come from both legitimate and non-legitimate origins. In general, this modus operandi is easily accessible especially when legitimate funds are used, and thus they do not trigger any suspicion when the bank account is opened. It appears that terrorist groups do not have specific challenges in hiding the real beneficiary of the funds or the exact purpose of the transaction (destination of funds) given that they may still include family members or relatives in the ownership chain. Concerning cash withdrawals, it may be more challenging if the terrorist organisation cannot access ATM-related to banks in

[1] http://www.ebf-fbe.eu/publications/statistics/

conflict zones. It requires at least basic planning and basic knowledge of how banking systems work. At the same time, once executed, cash withdrawals allow cross-border movements which make this risk scenario rather attractive.

Conclusions: terrorists groups use rather frequently this easily accessible modus operandi, although it requires some basic knowledge and planning capabilities to ensure that funds deposited are legitimate. The identity of the beneficiary of funds can be hidden. This modus operandi is rather attractive for terrorist groups. In that context, the level of TF threat related to deposits on accounts is considered as significant/very significant (level 3/4)

Money laundering

The assessment of the ML threat related to deposits on account /retail banking shows that this risk scenario concerns both placing funds and withdrawing funds (i.e. deposits on account and use of this account).

It is frequently used by organised crime organisations but also by relatives/close associates which extends the scope of the intent and capability analysis. Law enforcement authorities reported a frequent use of this modus operandi since it one of the easiest way to integrate illicit funds into the financial system. It does not require planning and knowledge of how banking systems work, and it is low cost. Also complex money laundering cases were reported with funds deposited on accounts transiting via a chain of complex operations. For such complex schemes, perpetrators may use available expertise from intermediaries.

Conclusions: the level of ML threat related to deposits on account is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to deposits on account /retail banking shows that as far as the placement and withdrawing of funds is concerned:

(a) risk exposure:
Deposits on accounts represent, by definition, high volumes of products where, in the case of cash, the origin of funds cannot be always traced. When traced through electronic payments, the origin of funds might be legitimate. In such case, the use made by those funds may trigger a link to terrorist activities. When used by terrorist organisations, funds may come from high risk third countries.

(b) risk awareness:
The risk awareness of credit and financial institutions is quite good due to the fact that the sector has put in place guidance to detect the relevant red flags on TF. While the sector is inherently highly exposed to TF risks, it has the adequate tools to detect these risks. This is confirmed by a good level of reporting. However, CDD and risk indicators are not always sufficient to detect a link to terrorist activities due to the legitimate origin of the funds. FIUs and LEAs are also well aware about the vulnerabilities of the sector and are proactively engaged with the sector. This is confirmed by the typology project launched by the Egmont group on ISIL. Nevertheless, some weaknesses remain in the supervision aspects.

(c) legal framework and controls
Retail banking services/deposits on accounts (including from cash) are covered by the

AML/CFT framework since the first AML/CFT legislation at EU level in 1991. Controls in place are generally considered as efficient. Obliged entities are applying CDD measures including monitoring and reporting of STRs in an effective way. It is nevertheless important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: although the risk exposure may be considered as quite high (significant level of transactions), the sector shows a good level of awareness to the risk vulnerability and is able to put in place the relevant red flags. The legal framework and controls are the basis of a good level of reporting. In that context, the level of TF vulnerability related to deposits on accounts/retail banking is considered as moderately significant (level 2).

Money laundering

The assessment of the ML vulnerability related to deposits on account /retail banking shows that it shares the same features as the TF vulnerability assessment.

(a) risk exposure:
Deposits on accounts represent, by definition, high volumes of products where in the case of cash, the origin of funds cannot be always traced. While rather common practice for credit and financial institutions, deposits represent a high number of operations that may involve different kind of customers (some may present factors of high risks, either because they are politically exposed persons or because they are based in areas identified as high risks).

(b) risk awareness:
The risk awareness is quite good due to the fact that the sector has put in place guidance to detect the relevant red flags on ML. While the sector is inherently highly exposed to ML risks, it has adequate tools to detect these risks. This is confirmed by a good level of reporting. FIUs and LEAs are also well aware about the vulnerabilities of the sector and are proactively engaged with the sector. Nevertheless, some weaknesses remain in the supervision aspects.

(c) legal framework and controls
Retail banking services provided by financial institutions and cash deposits to credit institutions are covered by the AML/CFT framework since the first AML/CFT legislation at EU level in 1991. Controls in place are considered as efficient. It is nevertheless important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: similarly to what has been analysed under the TF vulnerability part, deposits on accounts are less exposed to ML risks due to the good functioning of the controls and a good level of awareness from the sector. In that context, the level of ML vulnerability related to deposit on accounts/retail banking is considered as moderately significant (level 2).

Mitigating measures

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):
  (i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include

interconnection of beneficial ownership registers at EU level.

(ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements.

- The Commission will launch further analysis in order to identify risks and opportunities in FinTech/RegTech. The Commission FinTech Task Force will assess technological developments, technology enabled services and business models, will determine whether existing rules and policies are fit for purpose and will identify options and proposals to harness opportunities or address possible risks. .

- The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed.
- The ESAs should provide updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in financial institutions s. The Commission services will further analyse whether those guidelines allow a sufficient reinforcement of the position of the AML/CFT – compliance officer.

Institutional investment sector - Banking

Product
Deposits on accounts
Sector
Credit institutions - Institutional investment
General description of the sector and related product/activity concerned
The EU asset management sector is composed of two pillars that are complementing each other. The first pillar comprises the mutual fund industry, the so-called UCITS funds (EUR8 tr of assets under management). The second pillar includes alternative investment funds such as hedge funds, private equity, venture capital or real estate funds (EUR3 tr of assets under management).
Description of the risk scenario
Perpetrators are using institutional investors to invest in shares for integration of proceeds, title of shares to conceal beneficial ownership, frauds for predicate offence (e.g. insider dealing); brokerage accounts; investment to justify criminal proceeds as profit; predicate investment fraud. Placement of proceeds by using specialised, high-return financial services.
General comments
This risk scenario should be linked to the one related to institutional investment provided by brokers. It has been considered that as far as the ML vulnerability is concerned, the level of risk is higher for brokers.
Threat
Terrorist financing The assessment of the TF threat related to institutional investment- banks (securities, asset management, and investment) has been considered in conjunction with ML schemes related to institutional investment in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment. **Conclusion: in light of this, the assessment of the TF threat related to institutional investment through banks is considered as moderately significant (level 2).**
Money laundering The assessment of the ML threat related to institutional investment- banks (securities, asset management, and investment) shows that criminal organisations do not favour this kind of risk scenario. Although large amount of funds can be gathered through this process, it is not easy to access, not financially viable (depends on the quality of investment) and in any case, it requires knowledge and technical expertise. It is very close to wealth management financial services. However, perpetrators may have increased intention to use this modus operandi when they can rely on more complex planning carried out by facilitators for this type of services. **Conclusions: in that context, the assessment of the ML threat related to institutional investment through banks is considered as moderately significant (level 2).**

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to institutional investment - banks (securities, asset management, and investment) has been considered in conjunction with ML schemes related to institutional investment. In that context, the TF vulnerability does not benefit from a separate assessment.

Conclusion: in light of this, the assessment of the TF vulnerability related to institutional investment through banks is considered as moderately significant (level 2).

Money laundering

The assessment of the ML vulnerability related to institutional investment - banks (securities, asset management, and investment) shows that:

(a) risk exposure:
The inherent risk is potentially high due to the nature of customers. This sector is mostly exposed to high risk customers including PEPs. The volume of transactions concerned is significant, also in term of amounts with a high level of cross-border transactions.

(b) risk awareness:
According to FIUs, the level of STRs is quite low in respect to the volume of transactions concerned. At the same time, financial transactions concerned are more complex and the suspicious ones are probably less easy to detect by obliged entities. The fact that the service is provided by a credit institution limits the vulnerabilities given that credit institutions are obliged to fulfil a number of basic compliance requirements for all activities and apply the same level of controls whatever the financial services concerned. Nevertheless, based on the information received, it seems that supervisors could not show a sound understanding of the operational AML/CFT risks posed by this specific type of business activity.

(c) legal framework and controls:
Institutional investments through banks are covered by AML/CFT requirements at EU level. However, the quality of this legal framework's implementation is questionable. In the investment field, the client manager has a vested interest in conducting the business relationship (reward/salary) and this may lead him/her to margin of complaisance in the implementation of CDD. It is also important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: the risk exposure is inherently high due to the nature of the customer and the large amounts linked to the transactions. However, when provided by a bank, the investment service is quite well framed and controlled. The low level of STRs may be justified by the fact that due to the complexity of the transaction, few suspicious cases arose (in general, these transactions are approved by senior manager). In light of this, the ML vulnerability related to institutional investment provided through banking institutions is considered as moderately significant (level 2).

Mitigating measures

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting

forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):

(i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include interconnection of beneficial ownership registers at EU level.

(ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements

- The Commission will launch further analysis in order to identify risks and opportunities on FinTech/RegTech. The Commission FinTech Task Force will assess technological developments, technology enabled services and business models, will determine whether existing rules and policies are fit for purpose and identify options and proposals to harness opportunities or address possible risks. The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed.
- Updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in financial institutions should be provided by the ESAs and the Commission will further analyse whether those guidelines allow the position of the AML/CFT – compliance officer to be sufficiently reinforced.
- An analysis of operational AML/CFT risks linked to the business/business model in the institutional investment sector should be provided by the ESAs. .
- Further guidance for the application of beneficial ownership identification for providers of investment funds, especially in situations presenting a higher risk of ML/TF should be provided by the ESAs

Institutional investment sector - Brokers

Product

Deposits on accounts

Sector

Investments firms - Institutional investment

General description of the sector and related product/activity concerned

The EU asset management sector is composed of two pillars that are complementing each other. The first pillar comprises the mutual fund industry, so-called UCITS funds (EUR8 tr of assets under management). The second pillar includes alternative investment funds such as hedge funds, private equity, venture capital or real estate funds (EUR3 tr of assets under management).

Description of the risk scenario

Perpetrators are using institutional investors to invest in shares for integration of proceeds, title of shares to conceal BO, frauds for predicate offence (e.g. insider dealing); brokerage accounts; investment to justify criminal proceeds as profit; predicate investment fraud. Placement of proceeds by using specialised, high-return financial services.

General comments

This risk scenario should be linked to the one related to institutional investment provided by banks. It has been considered that as far as the ML vulnerability is concerned, the level of risk is lower for banks.

Threat

Terrorist financing

The assessment of the TF threat related to institutional investment - brokers (securities, asset management, and investment) has been considered in conjunction with ML schemes related to institutional investment - brokers. In that context, the TF threat does not benefit from a separate assessment.

Conclusion: in that context, the assessment of the TF threat related to institutional investment through brokers is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to institutional investment - brokers (securities, asset management, and investment) shows that criminal organisations do not favour this kind of risk scenario. Although large amount of funds can be gathered through this process, it is not easy to access, not financially viable (depends on the quality of investment) and in any case, it requires knowledge and technical expertise. It is very close to wealth management financial services. However, there may be intention when perpetrators can rely on more complex planning and use facilitators for this type of services.

Conclusions: in that context, the assessment of the ML threat related to institutional investment through brokers is considered as moderately significant (level 2).

Vulnerability
Terrorist financing The assessment of the TF vulnerability related to institutional investment-brokers (securities, asset management, and investment) has been considered in conjunction with ML schemes related to institutional investment - brokers. In that context, the TF vulnerability does not benefit from a separate assessment. **Conclusion: the risk exposure is inherently high due to the nature of the customer and the large amounts linked to the transactions. In addition, when provided by a broker/asset manager, the level of controls may be less efficient than when provided by a credit institution. In that context, the TF vulnerability related to institutional investment provided through brokers/asset managers is considered as significant (level 3).**
Money laundering The assessment of the ML vulnerability related to institutional investment -brokers (securities, asset management, and investment) shows that: **(a) risk exposure**: The inherent risk is potentially high due to the nature of customers. This sector is mostly exposed to high risk customers including PEPs. The volume of transactions concerned is significant, also in terms of amounts with a high level of cross-border transactions. **(b) risk awareness**: According to FIUs, the level of STRs is quite low in respect to the volume of transactions concerned. At the same time, the financial transactions concerned are complex and the suspicious transactions are probably less easy to detect by obliged entities. The fact that the service is provided by a broker affects the level of vulnerabilities which is considered as higher than the one concerning credit institutions. Competent authorities consider that asset managers are less equipped than credit institutions to detect suspicious transactions and apply the lowest controls on this kind of business relationships which constitute, most of the time, their core business. The competition component is not negligible and some cases have been identified where brokers accept to apply lower controls to attract more customers. Based on the information received, it seems that supervisors could not show a sound understanding of the operational AML/CFT risks posed by this specific type of business activity. **(c) legal framework and controls**: Institutional investments through brokers are covered by AML/CFT requirements at EU level. However, the quality of this legal framework's implementation is questionable. Competent authorities considered that the implementation of AML/CFT rules is less efficient for brokers than for credit institutions. In the investment field, the client manager has a vested interest in conducting the business relationship (reward/salary) and this may lead him/her to be more complacent in the implementation of CDD. **Conclusions: the risk exposure is inherently high due to the nature of the customer and the large amounts linked to the transactions. In addition, when provided by a broker/asset manager, the level of controls may be less efficient than when provided by a credit institution. In that context, the ML vulnerability related to institutional investment provided through brokers/asset managers is considered as significant (level 3).**

Mitigating measures

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):

(i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include interconnection of beneficial ownership registers at EU level.

(ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements

- The Commission will launch further analysis in order to identify risks and opportunities on FinTech/RegTech. The Commission FinTech Task Force will assess technological developments, technology enabled services and business models, will determine whether existing rules and policies are fit for purpose and identify options and proposals to harness opportunities or address possible risks. .

- The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed.
- Updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in financial institutions should be provided by the ESAs and the Commission will further analyse whether those guidelines allow the position of the AML/CFT – compliance officer to be to sufficiently reinforced.
- An analysis of operational AML/CFT risks linked to the business/business model in the institutional investment sector as well as further guidance for the application of beneficial ownership identification for providers of investment funds, especially in situations presenting a higher risk of ML/TF should be provided by the ESAs.
- A sufficient number of on-site inspections that is commensurate to the ML/TF risks identified should be conducted by supervisors. In this context, supervisors should assess the implementation of rules with regard to identification of beneficial ownership (compliance with the BO definition).
- Member States' supervisors should carry out within 2 years, a thematic inspection on institutional investment, with a particular focus on brokers, except for those that carried out recently such thematic inspections. The results of the thematic inspections should be communicated to the Commission**.**

Corporate banking sector

Product
Deposits on accounts
Sector
Credit institutions - Corporate banking
Description of the risk scenario
Perpetrators use cash front businesses to inject proceeds into legal economy using company accounts with multi-signatories
Threat
Terrorist financing The assessment of the TF threat related to corporate banking has been considered as in conjunction with ML schemes related to corporate banking in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment. **Conclusions: this modus operandi is used by criminals and, from LEAs perspective, requires only moderate levels of knowledge and expertise. In that context, the level of TF threat related to corporate banking is considered as significant (level 3).**
Money laundering The assessment of the ML threat related to corporate banking shows that this risk scenario has been recurrently used for ML schemes. While it requires more sophistication than the retail financial sector, depending on the financial service concerned, this level of sophistication is lowered (for instance, personal documentation is required only if there is demand for a credit loan). Nevertheless, given the level of sophistication that corporate banking operations require, in general the conduct of money laundering activities should involve the complicity of financial/legal intermediaries that shall be paid for their "services". This is a parameter that may have an impact on the intent component. **Conclusions: this modus operandi is used by criminals and, from LEAs perspective, requires only moderate levels of knowledge and expertise. In that context, the level of ML threat related to corporate banking is considered as significant (level 3).**
Vulnerability
Terrorist financing The assessment of the TF vulnerability related to corporate banking has been considered as in conjunction with ML schemes related to corporate banking. In that context, the TF vulnerability does not benefit from a separate assessment. **Conclusions: the level of TF vulnerability related to corporate banking is considered as moderately significant (level 2).**

Money laundering

The assessment of the ML vulnerability related to corporate banking shows that:

(a) risk exposure:
The inherent risk is potentially high due to the nature of customers. Indeed, corporate banking is, by definition, used by companies where the identification of the beneficial owner constitutes a particular point of vulnerability. The structure of the business relationship (more complex) and the transactions concerned (larger amounts than in retail payments) as well as the risk linked to forged documentation affect the level of risk exposure.

(b) risk awareness:
The sector appears quite aware of its risks. It has developed tools in order to trigger adequate red flags. FIUs have confirmed this element mentioning that a high number of STRs was received on this matter. Based on the information received, it seems that supervisors could not show a sound understanding of the operational AML/CFT risks posed by this specific type of business activity.

(c) legal framework and controls:
Corporate banking is covered by AML/CFT requirements at EU level. This framework is considered as satisfactory as the one covering other financial activities undertaken by credit institutions. It is also important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: corporate banking presents some vulnerability due to customers' risk factors. However, the legal framework in place is considered as adapted to these vulnerabilities and credit institutions involved in corporate banking activities are aware of the ML risks and equipped to address them. In that context, the level of ML vulnerability related to corporate banking is considered as moderately significant (level 2).

Mitigating measures

For the Commission

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):
  (i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include interconnection of beneficial ownership registers at EU level.

  (ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements
- Launching further analysis in order to identify risks and opportunities on FinTech/RegTech. The Commission set up a FinTech Task Force with the objective of assessing technological developments, technology enabled services and business models, determine whether existing rules and policies are fit for purpose and identify options and proposals to harness opportunities or address possible risks.
- The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed.

For the European Supervisory Authorities

- ESAs to provide for updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in financial institutions. The Commission will further analyse whether those guidelines allow the position of the AML/CFT – compliance officer to be sufficiently reinforced.
- In the context of the update of the Joint Committee of the ESAs' joint opinion on risks of ML and TF ESAs should provide an analysis of operational AML/CFT risks linked to the business/business model in the corporate banking sector.

For competent authorities/self-regulatory bodies

- Authorities/self-regulatory bodies should provide training sessions and guidance on risk factors with specific focus on non-face-to-face business relationships; off-shore professional intermediaries or customers or jurisdictions; complex/shell structures.
- Self-regulatory bodies/competent authorities should conduct thematic inspections on how beneficial owner identification requirements are implemented.
- Annual reports on the measures carried out to verify compliance by these obliged entities with their obligations related to customer due diligence, including beneficial ownership requirements, suspicious transaction reports and internal controls.
- Member States should put in place some mechanisms to ensure that the creation of structures should be carried out under control of a professional (obliged entity), who should have to develop their due diligence.
- Member States should put in place some mechanisms allowing competent authorities and FIUs to identify the situations where:
  (i) for legal entities: obliged entities have identified the senior manager as the beneficial owner, instead of the natural person who ultimately owns or controls the legal entity through direct or indirect ownership. In such case, obliged entities should keep record of any doubt that the person identified is the beneficial owner.

  (ii) for legal arrangements: obliged entities should identify cases where the settlor, trustee, protector, beneficiaries or any other natural person exercising ultimate control over the trust involve one or several legal entities. In such cases, the obliged entities should also identify the beneficial owner of these legal entities.
- Member States should put in place mechanisms to ensure the information held in central beneficial ownership register is verified on a regular basis. For this purpose, a national authority should be designated to collect and check the information on the beneficial owner. This national authority should receive from obliged entities any discrepancy that would be found between the beneficial ownership information held in the registers and the beneficial ownership information collected as part of their customer due diligence procedures. Where such discrepancies are not sufficiently justified by the legal structure or the legal arrangement, the national authority should provide for adequate pecuniary and/or administrative sanctions.
- Member States should ensure that services providers related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking are properly regulated and supervised at national level and comply with their obligations on beneficial ownership.

Private banking sector

Product
Deposits on accounts
Sector
Credit institutions- Private banking and wealth management
Description of the risk scenario
Perpetrators are using private banking and wealth management for investing in shares for integration of criminal proceeds, title of shares to conceal BO, frauds for predicate offence (e.g. insider dealing); brokerage accounts; investment to justify criminal proceeds as profit; predicate investment fraud. Placement of proceeds by using specialised, high-return financial services.
General comments
For this risk scenario, financial services concern high value investments and not the investments done by individuals in retail services.
Threat
Terrorist financing The assessment of the TF threat related to private banking (wealth management) has not been considered as relevant. In that context, the TF threat is not part of the assessment. **Conclusions: non relevant**
Money laundering The assessment of the ML threat related to private banking (wealth management) shows that this sector is used in connection with the following predicate offences: corruption and drug trafficking, fraud and tax evasion. This reduces the "scope" of organised crime organisations that may rely on this risk scenario. It requires some level of expertise that makes it not so easy to access and not very attractive (not financially viable). In particular, when dealing with private banking, the service is quite "high cost" (need of sufficient funds to access this financial service) and the business relationship less easy to establish. **Conclusions: from the above, the ML threat related to private banking is considered as moderately significant/significant (level 2- 3)**
Vulnerability
Terrorist financing The assessment of the TF vulnerability related to private banking (wealth management) has not been considered as relevant. In that context, the TF vulnerability is not part of the assessment. **Conclusions: non relevant**

Money laundering

The assessment of the ML vulnerability related to private banking (wealth management) shows that:

(a) risk exposure:
Private banking is generally exposed to high profile customers with a bigger risk appetite (PEPs in particular). It presents a higher geographical risk via establishment of branches in some third countries that do not have necessarily equivalent AML/CFT regimes to the EU AML/CFT framework.

(b) risk awareness:
According to FIUs, private banking is characterised by a very low (almost inexistent) level of STRs. As for investments services, institutions are sometimes competing between their commercial objectives and the need to fight against ML. The competition component is not negligible. It is worth mentioning that in this sector, the risk assessment is not always precise enough to ensure that the sector is aware of its risks, in particular risks linked to fraud and tax evasion. The supervision of activities at cross-border level is not considered as adequate. Based on the information received, supervisors could not show a sound understanding of the operational AML/CFT risks posed by this specific type of business activity.

(c) legal framework and controls:
Private banking is covered by AML/CFT requirements at EU level. Competent authorities consider that controls in place are not efficient. They explain this weakness by the fact that the quality of the controls depend on the financial culture of a country and that the understanding of the risks posed by this sector is not the same from one Member State to another. It is also important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: large amounts of transactions concerned and the fact that it implies high risk customers (PEPs) and potentially high risk areas (third countries with branches), the risk exposure is quite high. The low level of STRs shows that the controls in place are not necessarily adequate. However, there is a legal framework which establishes the basics of AML/CFT requirements. In that context, the level of ML vulnerability related to private banking is considered as significant (level 3).

Mitigating measures

For the Commission

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):
  (i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include interconnection of beneficial ownership registers at EU level.

  (ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements

- Launching further analysis in order to identify risks and opportunities on

FinTech/RegTech. The Commission set up a FinTech Task Force with the objective of assessing technological developments, technology enabled services and business models, determine whether existing rules and policies are fit for purpose and identify options and proposals to harness opportunities or address possible risks.

- The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed

For the European Supervisory Authorities (ESAs)

- ESAs to provide for updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in financial institutions. The Commission will further analyse whether those guidelines allow the position of the AML/CFT – compliance officer to be sufficiently reinforced.
- In the context of the update of the Joint Committee of the ESAs' joint opinion on risks of ML and TF, ESAs should provide an analysis of operational AML/CFT risks linked to the business/business model in the private banking sector.

For competent authorities

- Member States should ensure that supervisors conduct a sufficient number of on-site inspections that is commensurate to the ML/TF risks identified. In this context, supervisors should assess the implementation of rules with regard to identification of beneficial ownership (compliance with the BO definition).
- Member States' supervisory authorities should carry out a thematic inspection on private banking within 2 years, except for those that carried out recently such thematic inspections. The results of the thematic inspections should be communicated to the Commission.

Crowdfunding

Product
Crowdfunding
Sector
Crowdfunding platforms
General description of the sector and related product/activity concerned

Crowdfunding refers to an open call to the public to raise funds for a specific project. Crowdfunding platforms are websites that enable interaction between fundraisers and individuals interested in contributing financially to the project. Financial pledges can be made and collected through the platform.

The different business models that are used by crowdfunding platforms can be grouped into the following broad categories:

- Investment-based crowdfunding: Companies issue equity or debt instruments to crowd-investors through a platform.
- Lending-based crowdfunding (also known as crowdlending, peer-to-peer or marketplace lending): Companies or individuals seek to obtain funds from the public through platforms in the form of a loan agreement.
- Invoice trading crowdfunding: a form of asset-based financing whereby businesses sell unpaid invoices or receivables, individually or in a bundle, to a pool of investors through an online platform.
- Reward-based crowdfunding: Individuals donate to a project or business with expectations of receiving in return a non-financial reward, such as goods or services, at a later stage in exchange of their contribution.
- Donation-based crowdfunding: Individuals donate amounts to meet the larger funding aim of a specific charitable project while receiving no financial or material return.
- Hybrid models of crowdfunding: Combine elements of the other types of crowdfunding.

In a study commissioned by the Commission and published on 30 September 2015[2], data coverage from crowdfunding platforms across the EU was approximately 68% by EUR volume of the estimated total market size for the time period under consideration (2013-14).[3] Data covered loans, equity, rewards, donations and other crowdfunding models. As at 31 December 2014, 510 live platforms were active in the EU and 502 platforms were located in 22 Member States. Most platforms were located in the United Kingdom (143), followed by France (77) and Germany (65). The majority of platforms were involved in reward-based crowdfunding (30%), followed by platforms involved in equity crowdfunding (23%) and loan-based crowdfunding (21%).

[2] https://ec.europa.eu/info/sites/info/files/crowdfunding-study-30092015_en.pdf

[3] Coverage of both loans crowdfunding and equity crowdfunding was estimated at 81%.

Project data from the platforms amounted to a total of EUR 2.3 billion successfully raised in 2013-14.[4] The largest single projects raised EUR 6.1 million (equity) and EUR 5.0 million (loan). This compares with EUR 5 trillion of domestic outstanding bank loans to non-financial corporations in the EU at the end of 2014. Across the EU between 2013 and 2014, amounts raised through equity crowdfunding platforms grew by 167%, and amounts raised through loan crowdfunding platforms grew by 112%.
In 2014 the average amount raised was EUR 260 000 for equity crowdfunding and EUR 11 000 for loan crowdfunding. The average size of offers seems to be increasing. For example, the average amount raised through equity platforms grew by 21% (from EUR 215 000 to EUR 260 000).

Crowdfunding is an EU-wide phenomenon, as crowdfunding projects were identified in every Member State in 2013-14. However, there are significant differences in levels of activity between Member States. For equity crowdfunding projects located in the EU covered by the study, in 2013-14 the United Kingdom was the largest market by total amount raised (EUR 69 million), followed by France (EUR 14 million) and Germany (EUR 11 million). For loans crowdfunding projects covered by the study, in 2013-14 the United Kingdom was by far the largest market with EUR 1.6 billion, followed at a distance by Estonia (EUR 17 million) and France (EUR 12 million).

Cross-border project funding within the EU was EUR 102 million in 2013-14, less than 5% of total funding raised, of which EUR 15 million in cross-border financial return-based transactions.[5] However, it is likely that these amounts understate the true level of cross-border activity, as they only account for situations where the platform and the project are located in two different Member States (thus excluding situations where the provider of funds and the platform are located in two different Member States).

As far as the EU AML/CFT framework is concerned, it is not generally applicable to crowdfunding platforms as such - but it is applicable to specific types of crowdfunding services depending on the Business Models. According to the ESMA[6] Directive 2005/60/EC applies to firms including credit institutions and financial institutions, the latter including MiFID investment firms, collective investment undertakings and firms providing certain services offered by credit institutions without being one (including lending, money transmission, participation in securities issues and related services). As many platforms are currently operating outside the scope of MiFID they would not be automatically captured by the 3AMLD. However, the definition of 'financial institution' also includes those carrying out money transmission, participation in securities issues and the provision of services related to such issues, and safekeeping and administration of securities. Depending on the business model, this could capture some crowdfunding platforms. In addition, in the context

[4] Given the market coverage of the study, it can be estimated that a total of approximately EUR 3.4 billion was raised through crowdfunding across the European Union during 2013 and 2014 taken together, and EUR 2.2 billion was raised through equity and loans crowdfunding.
[5] Given the market coverage of the study, a total of approximately EUR 150 million of cross-border project funding can be estimated for the EU in 2013-14, of which EUR 19 million of equity and loans crowdfunding.
[6] https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1378_opinion_on_investment-based_crowdfunding.pdf

of its analysis of risks and risk drivers of lending-based crowdfunding, ESMA identified money laundering risks as one of those[7].

Description of the risk scenario

Perpetrators can create platforms to collect/accumulate funds and transfers them abroad for ML purposes or to finance terrorist attacks. This can be done by creating crowdfunding platforms directly linked to financial institutions or left to private initiatives on the internet. Crowdfunding platforms are set up under fictitious projects in order to allow collection of funds which are then withdrawn within the EU or transferred abroad. This could be used either to collect funds from legitimate sources for the purpose of terrorist financing – or to collect illicit funds from criminal activities using anonymous products.

Perpetrators post messages on the internet asking for donations in the form of prepaid mobile phone cards which are sold to raise funds; direct requests on Internet (via Tweeter) for specific amounts used ultimately for the purchase of illicit products.

Social media misuses (the so called "crowdsourcing") are another kind of risk scenario. Terrorists groups in particular have made use of social media and other online and mobile platforms to obtain funds which are channelled afterwards through different means of payment. This type of crowdsourcing is not further analysed in this fiche.

Threat

Terrorist financing:

Terrorist groups may have the intent to use the crowdfunding techniques to collect funds. Open sources information indicated that some cases were identified with regard to recent terrorist attacks. There are overall few cases where they have been used, and it covers usually smaller funds. Crowdfunding does not necessarily allow large amounts of funds to be raised which makes this risk scenario less attractive. In addition, suspicious activities are quite easier to detect and may deter terrorist groups from using this modus operandi as it is not the most secure option. However, if perpetrators invest more consequent planning, they could enable them to set up collection platforms allowing for more anonymous operations (use of strawmen or relatives) – which makes it more attractive.

Conclusions: there are some indicators that terrorist groups have used crowdfunding. It is not financially viable to raise or channel large amounts. It may be rather insecure compared to other types of services, or it requires more planning in order to hide the illicit intent. In that context, TF threat related to crowdfunding is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to crowdfunding shows that there is little to no evidence or indicators that criminals have used it to launder proceeds of crime. There are situations where criminals set up a company which is then used for crowdfunding activities but this requires some expertise and it can be costly. One case identified concerned a complex Ponzi scheme, using scam and fake projects. This confirms that this scenario is difficult to access and requires having access to payment processes. Nevertheless, while it requires some expertise, the intent is not negligible.

[7] https://www.eba.europa.eu/documents/10180/983359/EBA-Op-2015-03+%28EBA+Opinion+on+lending+based+Crowdfunding%29.pdf

Conclusions: criminals may have vague intentions to exploit this modus operandi which is not necessarily attractive and may be costly. In any case, it requires some expertise to be profitable. There is little evidence that it has been used. In that context, the level of ML threat related to crowdfunding is considered as lowly - moderately significant (level 1/2)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to crowdfunding shows that the sector cannot be assessed without taking other sectors into consideration.

(a) risk exposure:

The level of risk exposure varies depending on whether crowdfunding is directly linked to financial institutions or left to private initiatives on the internet. In both cases, it may imply the use of virtual currencies or (anonymous) electronic money which may constitute factors of vulnerabilities. Depending on the type of platform, the services may facilitate anonymous transactions – i.e. there may be limited or no CDD since the only requirements might be an e-mail address which can be opened without any controls, and the payments on the platform are made through an IP address in a location different than the user's address.

(b) risk awareness:

Even when a financial institution is involved, there is a lack of knowledge about the sources of funds, the scope of the funding and its purpose. When provided through private initiatives, crowdfunding services are out of the scope of any AML/CFT monitoring. Competent authorities, including at EU level, are aware that TF risks exist but the risk assessment is still incomplete at this stage to have a clear understanding of the risks. It is important to mention that where these platforms are included in the list of obliged entities, FIUs receive STR.

(c) legal framework and controls:

Crowdfunding as such is currently not covered by AML/CFT requirements at EU level. Hence there is no horizontal framework setting AML/CFT obligations for those services. Depending on the business model (e.g. UCITS), specific types of crowdfunding services may be covered by AML/CFT obligations – although those would not be the primary services for terrorist financing since it concerns more high value investment collections. Some Member States have covered crowdfunding platforms in their law through the transposition of the Payment Services Directive I. At this stage, 10 Member States have specific laws in place to cover crowdfunding platforms and 4 Member States adopted AML/CFT provisions. However, competent authorities consider that controls and supervisory actions are weak in particular given to the fact that many platforms are not established physically in the territory where they operate which hinders the efficiency of the controls. Where credit and financial institutions are involved, the effectiveness of controls is lower due to the fact that they can only rely on more limited information to monitor transactions and apply red flags. It is important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: the sector is not homogeneous and may interact with other sectors that can increase the level of vulnerabilities. Controls in place are not harmonised because there is no horizontal framework dealing with this issue. There are some concerns about the risk awareness of the sector. In that context, the level of TF vulnerability related to crowdfunding is considered as significant (level 3)

Money laundering

The assessment of the ML vulnerability related to crowdfunding shows similar vulnerability assessment as TF.

(a) risk exposure:

The level of risk exposure varies depending on whether crowdfunding is directly linked to financial institutions or left to private initiatives on the internet. In both cases, it may imply the use of virtual currencies or anonymous electronic money which may constitute factors of vulnerabilities. Depending on the type of platform, the services may facilitate anonymous transactions – i.e. there may be limited or no CDD since the only requirements might be an e-mail address which can be opened without any controls, and the payments on the platform are made through an IP address in a location different than the user's address.

(b) risk awareness:

The infiltration of such platforms by criminal organisations shall also be considered as an additional factor of vulnerability. Some LEAs and FIUs tend to consider that crowdfunding represents a widespread way to launder money. Even when a financial institution is involved, there is a lack of knowledge about the sources of funds, the scope of the funding and its purpose. When provided through private initiatives, crowdfunding services are out of the scope of any AML/CFT monitoring. Competent authorities, including at EU level, are aware that ML risks exist but the risk assessment is still incomplete at this stage to have a clear understanding of the risks. It is important to mention that where these platforms are included in the list of obliged entities, FIUs receive STR.

(c) legal framework and controls:

Crowdfunding as such is currently not covered by AML/CFT requirements at EU level. Hence there is no horizontal framework setting AML/CFT obligations for those services. Depending on the business model (e.g. UCITS), specific types of crowdfunding services may be covered by AML/CFT obligations. Some Member States have covered crowdfunding platforms in their law through the transposition of the Payment Services Directive I. At this stage, 10 Member States have specific laws in place to cover crowdfunding platforms and 4 Member States adopted AML/CFT provisions. However, competent authorities consider that controls and supervisory actions are weak in particular given to the fact that many platforms are not established physically in the territory where they operate which hinders the efficiency of the controls. In case credit and financial institutions are involved, the effectiveness of controls is lower due to the fact that they can only rely on more limited information to monitor transactions and apply red flags. It is important to mention that new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: the risk exposure is rather limited although large sums may be engaged in crowdfunding activities. Controls in place are not harmonised because there is no horizontal framework dealing with this issue. When regulated, these platforms are well aware of their risks and the level of reporting is quite good. The controls in place are still, sometimes, weak especially when obliged entities rely on limited information to carry out checks. In that context, the level of ML vulnerability is considered as significant (level 3).

Mitigating measures

- When applying article 4 of the 4AML Directive for extending the scope of obliged entities, Member States should consider the need to define crowdfunding platforms as obliged entities to be subject to AML/CFT requirements. Member States definitions of crowdfunding platforms should be aligned to the definition in the Commission's forthcoming legal framework – planned to be adopted in Q4 2017

Currency exchange

Product

Conversion of funds

Sector

Currency exchange offices

Description of the risk scenario

Perpetrators are converting their funds into another currency to facilitate the conversion, transfer or laundering of funds.

Threat

Terrorist financing

The assessment of the TF threat related to currency exchange shows that terrorist groups exploit this modus operandi, and especially foreign terrorist fighters. The conversion EUR/USD is particularly attractive for these groups. Bringing currency into conflict zones is one of the basic practices to finance the travels. From a technical point of view, the conversion of funds does not require specific planning, knowledge or expertise, and it's quite easy to access. Although it does not consist in the raising or transferring of funds, it is a necessary step for moving physically "clean" currency (most of the time in cash). Terrorist groups may consider that the exchange of currency is as attractive as the collection or the transfer of funds to finance their activities.

Conclusions: terrorist groups show some intent and capability to use currency exchange to sustain/carry out their operations. This scenario does not require specific planning or expertise and has been used already. In that context, the level of TF threat related to currency exchange is considered as significant (level 3).

Money laundering

The assessment of the ML threat related to currency exchange shows that there are some cases where currency exchange offices have been infiltrated by criminal organisations to run their activities. This is particularly relevant in offices operating in airport zones. High volumes of money can be easily converted and make the access to "clean" currency easy for these criminal organisations. Similarly to TF, the currency exchange does not require specific planning or expertise for ML purposes. However, currently, the volume of suspicious transactions is difficult to assess.

Conclusions: although the volume of cases is difficult to assess by law enforcement authorities, the indicators show that criminal organisations may use currency exchange to launder proceed of crime. This scenario does not require specific planning or expertise and has already been used. In that context, the level of ML threat related to currency exchange is considered as significant (level 3)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to currency exchange shows that the vulnerability is present whatever the type of transaction concerned:
- the customer gives sums in cash and orders to exchange this cash for a currency that has to be transferred to an indicated bank or payment account.
- the currency exchange is performed on the internet and transferred, electronically, to an indicated bank account or payment account.

(a) risk exposure:
The fact that currency exchange offices deal most of the time with transactions in cash is a factor indicating a higher vulnerability. This is amplified when large denomination notes are involved, and these are not properly monitored. LEAs and competent authorities have noticed that PEPs are also common users of currency exchange.

(b) risk awareness:
In the different risks scenarios where currency exchange offices are used, MVTS providers or bank/payment institutions are associated to these offices. The consequence is that currency exchange offices tend to rely on the underlying MVTS providers or on the bank/payment institution to conduct the customer due diligence measures. In this context, the currency exchange office/platform is not able to get the full picture of the business relationship. Despite factors of high exposure, the level of STRs remains low except in specific cases, such as USD conversion requested from high risk third countries (e.g. Syria), It seems that the sector does not show awareness to TF risks.

(c) legal framework and controls:
Currency exchange offices are covered by the AML/CFT framework at EU level. There is little information concerning the level of controls which vary a lot from one Member State to another. Some Member States have dedicated AML/CFT compliance departments dealing with currency exchange offices but this practice is not widespread enough to draw concrete consequences. In particular when carrying occasional transactions, currency exchange offices have to apply CDD only for occasional transactions beyond EUR 15 000 under 3AMLD. This threshold is relatively high, especially in the context of terrorism financing risks where low amounts are at stake.

Conclusions: the awareness of the sector to TF risk is low and relies too often on the due diligence conducted by associated sectors, such as MVTS or bank/payment institutions. High risk customers and countries are recurrently involved in such transactions. The legal framework in place does not have an influence on the level of STRs. In that context, the level of TF vulnerability related to currency exchange is considered as significant (level 3).

Money laundering

The assessment of the ML vulnerability related to currency exchange shows that:

(a) risk exposure:
The fact that currency exchange offices deal most of the time with transactions in cash is a factor indicating a higher vulnerability. This is amplified when large denomination notes are involved, and these are not properly monitored. LEAs and competent authorities have

noticed that PEPs are also common users of currency exchange. Currency offices in boarder zones are more vulnerable than other offices.

(b) risk awareness:
In the different scenarios where currency exchange offices are used, MVTS providers or bank/payment institutions are associated to these platforms. The consequence is that currency exchange offices tend to rely on the underlying MVTS providers or on the bank/payment institution to conduct the customer due diligence measures. In that context, the currency exchange office is not able to get the full picture of the business relationship. For AML purposes, the level of reporting is uneven from one Member State to another, and does not necessarily consist in STR (mostly CTR).

(c) legal framework and controls:
Currency exchange offices are covered by the AML/CFT framework at EU level. The regulation and the supervision of the sector is usually not considered as robust enough, and is less efficient than for other financial institutions. In particular, when carrying occasional transactions, currency exchange offices have to apply CDD only for occasional transactions beyond EUR 15 000 under 3AMLD. This threshold seems relatively high, which explains why Member States usually applied lower thresholds at national level. Such variety of thresholds for occasional transactions by currency exchange offices may have a negative effect from an internal market perspective.

Conclusion: awareness of the sector is rather uneven, and controls in place are not efficient given the low level of reporting. Competent authorities do not consider that the regulation and the supervision work effectively. In that context, the level of ML vulnerability related to currency exchange is considered as significant. (level 3)

Mitigating measures

- Member States should ensure that supervisors conduct a sufficient number of on-site inspections that is commensurate to the ML/TF risks identified.
- Competent authorities should provide further risk awareness and risk indicators relating to terrorist financing.
- Member States should define a threshold below EUR 15 000 triggering CDD obligations in case of occasional transactions, which is commensurate to the AML/CFT risk identified at national level. Member States should report to the Commission such threshold applicable to occasional transactions defined at national level. A threshold similar to the one for occasional transactions for transfers of funds as defined in article 11(b)(ii) of 4AMLD is considered as commensurate to the risk (i.e. EUR 1 000).

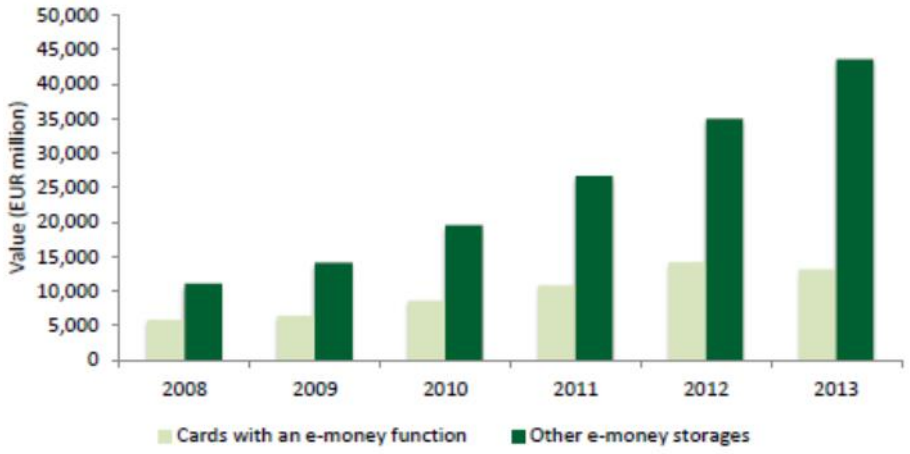
E-money sector

Product
E-money
Sector
Credit and financial institutions
General description of the sector and related product/activity concerned
'Electronic money' is defined under the second E-Money Directive (EMD2, 2009/110/EC) as electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer. A key characteristic of e-money is its pre-paid nature. This means that an account, card, or a device needs to be credited with a monetary value in order for that value to constitute e-money. Examples of e-money are money stored on cards, money stored on mobile devices, and money stored in online accounts. Depending on the way e-money is stored, it can be classified as 'hardware-based' or 'server-based'. Certain e-money products require identification of the owner, others allow owners to remain anonymous Prepaid cards can have many different features, including reloadable and non-reloadable functionalities; cards linked to other e-money schemes (i.e. cards linked to online accounts); or cards with basic bank account features (also known as IBAN cards), which can accept incoming bank transfers in order to credit the card balance. Other potential distinctions between e-money products can include the manner in which e-money is created or issued. The key distinction relates to whether e-money can be pre-paid by the user (payer) or by a third-party on behalf of or in favour of the payer (e.g. company in case of business-to-business (B2B) cards or by a merchant in multi-merchant loyalty schemes). It is also linked to the question of whether an e-money product allows for reloading (i.e. ability to add more value to the product after the initial issuing of e-money by the issuer). Yet another distinction could also be made between personalised and non-personalised products. Not all monetary value that is stored electronically should be considered as e-money in the context of the EMD2. Limited network products such as gift cards and public transport cards that can only be used with a certain retailer or a chain of defined retailers are outside the scope of EMD2. Also, virtual currencies such as Bitcoin are not considered as e-money as they do not represent monetary value. **Description of the sector** In the landscape of e-money, prepaid cards and e-wallets are predominant. As regards the use of e-money for making payment transactions, there is a clear increasing trend in the use of account based e-money products as compared to card based products. Looking into the future, growth is primarily expected in the area of digital wallets used for e-commerce payments (i.e. Google Wallet). With regard to technological developments, increased usage of NFC (Near Field Communication) technology allowing for contactless payments using mobile phones, is expected. Systematic examination of the market in terms of volume and value of e-money transactions is more complex. Although the European Central Bank (ECB) serves as a central source of statistical data on the value and volume of e-money transactions, there are numerous data

gaps. According to the ECB, this is mainly due to the fact that only Eurozone Member States are required to report statistical information, with remaining Member States doing this voluntarily.

Although existing ECB statistics do not provide a full picture of the size of the e-money market, they provide some indications concerning the orders of magnitude related to the market size, as well as changes over time.

Figure 6 - Value of e-money transactions in the Eurozone by type



Note: For cards with an e-money function the figure does not include data for Estonia, Finland, Greece, Latvia, Malta, Slovenia, and historical data for Slovakia. For other e—money storages the figure only includes data for Cyprus, Greece, Italy. Luxembourg, Slovakia, and recent data for Slovenia

Source: Own analysis based on ECB data. Status as of October 2014.

According to the ECB data on the e-money market, in 2014, e-money payment transactions for the 22 Member States that provided data amounted to EUR73 billion corresponding to e-money payment transactions with e-money issued by EU resident payment service providers. This amount of EUR73 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 and therefore underestimate the actual size of the EU market. The average transaction value on that basis was of EUR35. 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 EUR19.3 billion[8], 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 largest 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.

Relevant actors

Electronic money can be issued by credit institutions, electronic money institutions and post

[8] Estimate obtained by subtracting from the global figure provided by the ECB (EUR73 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. EUR3.3 billion.

office giro institutions where they have a licence to do so. Also the European Central Bank, national central banks and Member States with their regional or local authorities when acting in their public capacity are allowed to do so.
A recent, not yet published, study commissioned by the Commission, has identified that **in 2014, 177 e-money institutions (EMIs) were licenced EU wide** to issue e-money, the majority of them being in the UK and DK, NL, LV, BE, CZ. No EMIs were identified in AT, EE, GR, IE, PO, PT, SK, SI.
As regards the different business models used for the issuance of e-money, three types of actors are recognised in EMD2:

- **the issuer:** entity which 'sells' e-money to the customer (whether a consumer or a business) in exchange for a payment. It is also the entity that requires authorisation to issue electronic money and is regulated by EMD2;
- **the distributor:** entity other than the issuer that can distribute or redeem e-money on behalf of the issuer (i.e. it re-sells the e-money issued by the issuer, such as a retail outlet selling prepaid cards);
- **the agent:** entity that acts on behalf of the EMI through which an EMI can carry out payment services activities in another Member State (except for issuing e-money) without establishing a branch in that Member State.

In practice, this distinction appears to be used by the consulted EMIs primarily in the context of cross-border provision of e-money services, with selected EMIs using 'distribution partners' in order to operate in other Member States.

Description of the risk scenario

Perpetrators use characteristics and features of some of new payment methods "directly" using truly anonymous products (i.e. without any customer identification) or "indirectly" by abusing non-anonymous products (i.e. circumvention of verification measures by using fake or stolen identities, or using straw men or nominees etc.)
Perpetrators can load multiple cards under the anonymous prepaid card model. This multiple reloading could lead to substantial values which can then be carried out abroad with limited traceability.

Threat

Terrorist financing
The assessment of the TF threat related to e-money shows that the use of e-money can be particularly attractive for terrorist groups, as it allows funds to be moved easily and anonymously (in particular with prepaid cards instead of bulk of cash). In practice, e-money is rather easy to access and does not require specific expertise or planning. This is even more the case for non-account based e-money products. As far as the use for TF purposes is concerned, LEAs have gathered evidence that e-money loaded onto prepaid cards has been used to finance terrorist activities, in particular to assist the terrorists in committing their actions (hotel or car rentals).
However, the level of TF threat presented by e-money shall be assessed proportionally to the level of threat represented by cash which constitutes a more competitive and more attractive tool because it is easier to access than e-money. In that sense, cash is still the preferred option to finance travels to war zones. At the same time, e-money loaded onto prepaid cards may be seen by terrorist groups as more secure as it allows more discrete payments than cash. They may also see this option as more attractive when cash transactions are not an available option (e.g. online transactions, online purchases).

Conclusions: e-money is attractive for terrorist groups, especially when loaded onto prepaid cards, as it allows terrorist activities to be financed easily and with a low level of planning/expertise. LEAs have evidence that this modus operandi has been used recurrently. However, it seems that it is still less attractive than cash. In that context, the level of TF threat related to e-money is considered as significant/very significant (level 3/4).

Money laundering

The assessment of the ML threat related to e-money shows that the volume of transactions concerned is high and this modus operandi is quite attractive for criminal organisations, including non EU ones who want to operate in the EU. This is particularly the case for e-money carried out via prepaid cards.

FIUs have detected multiples cases of misuses of e-money (tax fraud, drug trafficking, prostitution) through the purchase of multiple prepaid cards of large amounts (sometimes above EUR600). LEAs have noticed cases where the proceeds of drug trafficking were laundered by prepaid cards. Prepaid cards may allow large amounts of funds to be easily brought (some cards have no limit).

As for TF, the intent to use cash remains nevertheless higher than using e-money.

Conclusions: similarly to TF, e-money is attractive for criminal organisations and terrorist groups, especially when loaded onto prepaid cards, as it can easily allow money laundering and requires a low level of planning/expertise. The intent is quite high, while the capability of criminal organisations to use e-money is still higher for cash than for e-money. In light of this, the level of ML threat related to e-money is considered as significant/very significant. (level 3/4).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to e-money shows that:

(a) risk exposure:

Due to the fact that some e-money products may, in certain circumstances, entail anonymous transactions, the risk exposure of the sector is high. E-money products are nowadays widespread means of payment which can generate significant volumes of financial flows in a speedy and sometimes anonymous way, including cash-based which may have cross-border functionalities. Based on new technologies, inherent risks of e-money depend on the structure of the product, the nature of the operator and its capability in managing these new technologies to effectively identify and report suspicious transactions. Regulators and supervisors have noticed that this capability is uneven from one operator to another. The fact that e-money does not necessarily involve high amounts is rather irrelevant in the context of terrorist financing, due to the often low costs of carrying out terrorist activities.

(b) risk awareness:

The promotion of e-money products in the field of financial inclusion or vulnerable people impacts the risk awareness of the sector which tends to consider TF abuses as marginal. Thus, the sector tends to advocate that due to the low level of TF risks, simplified CDD is adequate. Where CDD is exempted (i.e. where no identification and no verification is performed), the monitoring of the transaction is not considered as sufficient to identify suspicious transactions and to process reporting of the transactions (no data linked to the

transaction). The risk awareness tends nevertheless to increase. Some big players of the e-money market have developed robust risk assessments in order to better identify and understand the risks that the sector faces. They also improved awareness focused on CTF compliance and auditing, through information sharing and training. In addition, there are increasing initiatives aimed at engaging with competent authorities and LEAs. Some Member States have already included in their national AML/CFT framework some mitigating measures to limit the risks posed by the anonymity (for instance transactions still recorded when processed through the internet or the possibility to keep track of the IP addresses). However, from a more general point of view, the sector is still not harmonised and small players tend to have limited resources to provide guidance, training or dedicated staff. Based on the information received, it seems that supervisory authorities have a limited understanding of the TF risks to which the e-money sector is exposed.

(c) legal framework and controls

E-money is covered by AML/CFT requirements at EU level. Under the current AML/CFT framework, e-money products benefit from an exemption regime which allows CDD not to be applied when specific conditions are fulfilled (EUR250 for non-reloadable e-money or EUR 2500 for reloadable e-money). The inclusion of e-money in the EU AML/CFT framework has played a role in increasing the suspicious transactions reports. However, many electronic money institutions operate across borders in the EU. In that context, the supervision of the sector is not considered as sufficiently robust to address the TF risk. It appears that the anonymity of the product is a feature meant to attract customers – a feature which is then compensated by the monitoring of transactions; however this approach raises doubt regarding the effectiveness of AML/CFT framework in the absence of identification measures. Finally, new risks and opportunities may emerge with FinTech/RegTech.

Conclusions: when used anonymously, e-money is inherently exposed to TF vulnerability. The level of awareness of the sector is growing but not in a sufficient way to allow FIUs to acquire enough data from suspicions transactions. In that context, the level of TF vulnerability related to e-money is considered as significant/very significant. (level 3/4)

Money laundering

The assessment of the ML vulnerability related to e-money shows that:

(a) risk exposure:

Due to the fact that some e-money products may, in certain circumstances, entail anonymous transactions, the risk exposure of the sector is high. E-money products are nowadays widespread means of payment which can generate significant volumes of financial flows in a speedy and sometimes in an anonymous way, including cash-based which may have cross-border functionalities. Based on new technologies, inherent risks of e-money depend on the structure of the product, the nature of the operator and its capability in managing these new technologies to effectively identify and report suspicious transactions. Regulators and supervisors have noticed that this capability is uneven from one operator to another.

(b) risk awareness:

The promotion of e-money products in the field of financial inclusion or vulnerable people impacts the risk awareness of the sector which tends to consider ML abuses as marginal. Thus, the sector tends to advocate that due to the low level of ML risks, simplified CDD is

adequate. Where CDD is exempted (i.e. where no identification and no verification is performed), the monitoring of the transaction is not considered as enough to identify suspicious transactions and to process reporting of the transactions (no data linked to the transaction). The risk awareness tends nevertheless to increase. Some big players of e-money market have developed robust risk assessments in order to better identify and understand the risks that the sector faces. They also improved awareness focused on AML compliance and auditing, through information sharing and training. In addition, there are increasing initiatives aimed at engaging with competent authorities and LEAs. Some Member States have already included in their national AML/CFT framework some mitigating measures to limit the risks posed by the anonymity (for instance transactions still recorded when processed through the internet or possibility to keep track of the IP addresses). However, from a more general point of view, the sector is still not harmonised and small players tends to have limited resources to provide guidance, training or dedicated staff. Based on the information received, it seems that supervisory authorities have a limited understanding of the TF risks to which the e-money sector is exposed.

(c) legal framework and controls:

E-money is covered by AML/CFT requirements at EU level. Under the current EU AML framework, e-money products benefit from an exemption regime which allows CDD not to be applied when specific conditions are fulfilled (EUR250 for non-reloadable e-money or EUR 2500 for reloadable e-money). The inclusion of e-money in the EU AML/CFT framework has played a role in increasing the suspicious transactions reports. However, LEAs and competent authorities tend to consider that the controls in place are not efficient enough and that e-money remains, from the elements gathered during criminal investigations, a tool used by criminal organisations (using anonymous products or products subject to simplified due diligence). It appears that anonymity of the product is a feature meant to attract customers – a feature which is then compensated by the monitoring of transactions; however this approach raises doubts regarding the effectiveness of AML/CFT framework in the absence of identification measures. Concerning supervision, the situation is rather similar to that of other payment institutions (see relevant fiche) – noting ESAs stressed weaknesses in this sector for managing ML risks associated with technological advances and financial innovation. Finally, the recent adoption of Directive 2014/92/EU on access to payment accounts (due to be transposed by September 2016) is an important element to take into consideration in the context of the financial inclusion aspects. New risks and opportunities may emerge with FinTech/RegTech.

<u>Conclusions:</u> e-money is inherently exposed to ML vulnerability when used anonymously. While the level of awareness of the sector to ML risks seems higher than for TF, the structure of the sector and its capability to provide for dedicated resources and training is quite low. The level of STRs confirmed this point. The legal framework in place has increased the controls applied in this sector, but these controls remain inadequate (monitoring only). In that context, the level of TF vulnerability related to e-money is considered as <u>moderately significant/ significant</u> (level 2/3).

Mitigating measures

- The Commission proposes in its proposal for amending Directive (EU) 2015/849 (COM(2016)450) to (i) lower (from 250 to 150 EUR) the thresholds in respect of non-reloadable pre-paid payment instruments to which such CDD measures apply and (ii) suppress the CDD exemption for online use of prepaid cards. This will better

serve identification purposes and widen customer verification requirements. Limiting the anonymity of prepaid instruments will provide an incentive to use such instruments for legitimate purposes only, and will make them less attractive for terrorist and criminal purposes.

- In the context of the update of the Joint Committee of the ESAs' joint opinion on risks of ML and TF, ESAs should provide an analysis of operational AML/CFT risks linked to the business/business model in the e-money sector.

Transfers of funds

Product

Transfers of funds

Sector

Credit and financial institutions –Money value transfer services (MVTS)

General description of the sector and related product/activity concerned

Money value transfer or money remittance is defined under PSD2 as a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.
A key example of money remittance is the remittances service offered by large agency network providers (Money Value Transfer Systems or MVTS) where the payer gives cash to a payment service provider's agent to make it available to the payee through another agent.
Statistics:

Money remittance is a payment service that can be provided by banks, e-money institutions and authorised payment institutions (APIs). Money remittance is the payment service for which APIs are most commonly authorised for (40% of all authorisations).

According to the report on the Payment Services Directive of London Economics and *IFF* in association with PaySys, in 2012[9] there were 568 authorised payment institutions in the EU (considering the Payment Institutions registers and additional information provided by competent authorities) out of which 330 were specifically authorised to provide money remittance services.

Regarding the ECB payment statistics, these are the relevant statistics per reporting country on money remittance:

[9] http://ec.europa.eu/internal_market/payments/docs/framework/130724_study-impact-psd_en.pdf

MS	Total number of money remittance transactions sent in 2014 (millions)	Total value of money remittance transactions sent 2014 (EUR billion)	Total number of cross-border money remittances received in 2014 (millions)	Total value of cross-border money remittances received 2014 (EUR billion)
BE	0.35	1.56	0.18	0.02
DE	13.01	155.48	0.40	0.44
EE	-	-	-	-
IE	0.11	1,014.23	0.12	1,014.23
EL	0.35	1,249.35	0.00	0.00
ES	12.71	3.57	0.27	0.07
FR	0.32	0.86	0.01	0.09
IT	2.67	1.31	0.20	1.31
CY	0.48	149.83	0.05	22.77
LV	0.83	1,006.72	1.15	244.05
LU	0.00	0.00	0.00	0.00
MT	-	-	-	-
NL	-	-	-	-
AT	0.47	0.40	0.03	0.03
PT	-	-	-	-
SI	16.08	1,542.44	-	-
SK	0.04	11.51	0.27	66.43
FI	-	-	-	-
BG	39.81	3,144.74	0.99	556.08
CZ	-	-	-	-
DK	-	-	-	-
HR	0.12	0.19	0.27	0.59
LT	-	-	-	-
HU	0.06	6.85	0.16	13.57
PL	-	-	-	-
RO	0.00	0.00	0.00	0.00
SE	-	-	-	-
UK	-	-	-	-

In addition, it could also be pointed out that all countries have some type of estimate on workers' remittances (defined as current private transfers from migrant workers who are

considered residents of the host country -i.e. non-residents of the home economy- to recipients in the workers' country of origin) from either the World Bank Migration and Remittances Factbook or Eurostat, with the notable exception of Denmark and the UK which do not collect remittances data at all. According to some general figures of the World Bank on 2012, this type of global workers´ remittances were then estimated $ 514 billion of which $401 billion were sent to developing countries (World Bank Report 2012), with a growth rate of more than 10% per year.

The market landscape shows that different types of MVTS providers are operating. This is reflected in the Payment Services Directive, which provides for "registered MVTS" and "authorised MVTS".

Description of the risk scenario

ML: Perpetrators may use MVTS services:

- to comingle funds from legitimate/illegimate customers (fake ID, fake invoices, …)

- to launder proceeds of crime through settlement systems in a third country (using passporting). MVTS channel funds through highly complex payment chains with a high number of intermediaries and jurisdictions involved in the funds circuit, thereby hindering traceability of illicit funds. MVTS operating throughout the payment chain often establish formal and/or informal settlement systems (frequently along with trade-based money laundering techniques) also hampering traceability of illicit funds.

- to break large sums of cash into smaller amounts that can be sent below the thresholds where stricter identification of the customer is required

- to place the proceeds of crime into the financial system through the regulated MVTS offering payment accounts or similar products. Perpetrators may also use such regulated MVTS providers to channel their funds

- to place and/or transfer their funds, through money remittance services. Risks of ML/TF activity may be particularly high when funds to be transferred are received in cash or in anonymous e-money

TF: Perpetrators use money and value transfers services provided by financial institutions to place and/or transfer funds that are in cash or in anonymous e-money (non-account based transactions). They use MVTS services to transfer rapidly amounts across jurisdictions, usually favouring a series of low amounts transactions to avoid raising red flags.

Threat

Terrorist financing

The assessment of the TF threat related to money value transfers services shows that terrorist groups recurrently use this modus operandi. LEAs and FIUs have gathered strong evidence that these services are used to collect and transfers funds which support the financing of terrorist activities, both within the EU and in particular to transfer funds by/for foreign terrorist fighters travelling to/from the conflict zones. MVTS are, depending on their organisation, easy to access and terrorists do not require specific expertise or techniques to abuse this service for finance terrorist activities. Terrorists might be more attracted to use large MVTS due to its global network of agents, whilst smaller MVTS might not be so attractive since they usually operate in a limited number of countries. Due to their features (see vulnerabilities part), MVTS are perceived as attractive and secure.

Conclusions: MVTS are recurrently used to finance terrorist activities and do not require specific knowledge or planning. In light of this, the level of TF threat related to

MVTS is considered as very significant (level 4).

Money laundering

The assessment of the ML threat related to money value transfers services does not differ from that of TF. Organised crime groups recurrently use this modus operandi. LEAs and FIUs have gathered strong evidence that these services are used to collect and transfers funds which support the activities of money laundering. MVTS are, depending on their organisation, easy to access and do not require specific expertise or techniques to launder proceeds of crime. Due to their features (see vulnerabilities part), MVTS are perceived as attractive and secure.

Conclusions: MVTS are recurrently used to launder money and do not require specific knowledge or planning. In light of this, the level of ML threat related to MVTS is considered as very significant (level 4).

Vulnerability

The assessment of the TF vulnerability related to money value transfers services presents, for several aspects, similarities with ML vulnerability assessment.

(a) risk exposure:
Reliance on cash based transactions and the recurring use of these services in high risk areas lead to a high risk exposure.

(b) risk awareness:
According to the competent authorities, the risk awareness of the sector has recently increased (due to the recent terrorist attacks) but the suspicious transactions remain difficult to detect because of the low amounts at stake. The level of reporting varies a lot and depends on the size of the MVTS provider. Big players may report more than small players, who rarely report back to FIUs according to FIU feedback. However, LEAs notice that the bigger players are more misused by terrorists than the smaller ones. There is a lack of information sharing between branches (due to personal data restrictions) which may impede national authorities in identifying suspicious actors related to a suspect which take place between two third countries.

(c) legal framework and controls
Registered and authorised MVTS are subject to AML/CFT requirements at EU level. The controls in place are considered as inadequate by competent authorities, in particular in the context of cross-border transactions, to address TF risks. Because of the reliance on agents, the supervision of the sector is very challenging: supervisors find it difficult to monitor what agents are doing in term of compliance with CDD requirements. Currently, the cross-border cooperation is not working properly and supervisors are not able to appropriately put in place the controls and the sanctions regime. In addition, when carrying out occasional transactions, MVTS providers have to apply CDD only for occasional transactions beyond EUR15 000 under 3AMLD. This threshold seems relatively high, especially in the context of terrorism financing risks where lower amounts are at stake.

Conclusions: MVTS vulnerability to TF is similar to MVTS vulnerability to ML. Even if the private sector is more aware about the risk of being abused for TF purposes, the

detection of suspicious transactions remains difficult due to the low amounts concerned. The cross-border exchange of information is still challenging, in particular due to the reliance on agents. In light of this, the level of TF vulnerability related to MVTS is considered as <u>significant/very significant (level 3/4).</u>

<u>Money laundering</u>

The assessment of the ML vulnerability related to money value transfers services cannot be undertaken without considering that most of the MVTS rely on agents. In the context of MVTS, agents constitute the main factor for risk exposure. They are, in addition, difficult to control and supervise.

a) risk exposure:
MVTS services are, in a number of cases, cash based and allow for anonymous and speedy transactions. Due to their features and in particular the reliance on agents, they can be provided in high risk third countries and may be used by high risk customers which are meant to be subject to specific monitoring and controls. Usually MTVS provide non-account based transfers of funds, therefore there is no lengthy financial relationship but only a series of isolated transactions, for which the only form of CDD consists in recording the formal identification data of the clients. This feature, together with the possibility of identity frauds, makes it also possible to use "straw persons", so that no information about the real individuals behind the transactions (senders/receivers) or the purpose of the transactions themselves is detectable.

b) risk awareness:
Competent authorities and FIUs consider that the understanding of the risk within the MVTS sector is not high enough and that the customer due diligence measures undertaken are too weak. IT systems are mostly in place at the level of the group, but agents are not aware of the risks and of the adequate level of CDD to be applied. LEAs have noticed the recurrent use of fake ID and repeated occasional transactions to support ML schemes and which undermine the sector's capability to detect suspicious transactions. Consequently, FIUs also find difficulties in detecting and analysing the risk. The organisational framework of the MVTS is, by definition, not centralised as these services may be provided by non-bank operators which are difficult to reach, to provide some guidance or training.

c) legal framework and controls:
Registered and authorised MVTS are subject to AML/CFT requirements at EU level. However, still because of the reliance on agents, the supervision of the sector is really challenging: supervisors find it difficult to monitor what agents are doing in terms of compliance with CDD requirements. Currently, cross-border cooperation is not working properly and supervisors are not able to appropriately organise the controls and the sanctions regime. In addition, when carrying out occasional transactions, MVTS providers have to apply CDD only for occasional transactions beyond EUR15 000 under 3AMLD– which limits the effect of CDD rules applied in the sector.

<u>Conclusions</u>: whilst the risk exposure of the MVTS sector is high, the risk awareness is quite low because of the lack of a centralised organisational framework. The reliance on agents constitutes a factor of vulnerability which hampers the supervision and the controls. The legal framework in place is not comprehensive enough to address issues

such as the cross-border cooperation or supervisory actions on the agent. In that context, the level of ML vulnerability related to MVTS is considered as <u>significant/very significant</u> (level 3/4).

Mitigating measures

- The 4AMLD will reinforce CDD measures with regard to occasional transactions for funds transfer (threshold of EUR1 000 applicable for transfers of funds – which triggers CDD obligations).
- In the context of the update of the Joint Committee of the ESAs' joint opinion on risks of ML and TF, ESAs should provide an analysis of operational AML/CFT risks linked to the business/business model in the MVTS sector.
- Member States should ensure that supervisors conduct a number of on-site inspections commensurate to the level of ML/TF risks identified. These inspections should include a review of training carried out by agents of obliged entities.
- Member States' supervisors should carry out a thematic inspection in the MVTS sector within 2 years, with the exception of those that recently carried out such thematic inspections. The results of the thematic inspections should be communicated to the Commission.
- In addition, competent authorities should provide further risk awareness and risk indicators relating to terrorist financing to the MVTS sector. The obliged entities should provide mandatory training to agents to ensure that they are aware about their AML/CFT obligations and how to detect suspicious transactions.
- Pending the application of 4AMLD, Member States should define a threshold below EUR15 000 triggering CDD obligations in case of occasional transactions, which is commensurate to the AML/CFT risk identified at national level. A threshold similar to the one for occasional transactions for transfers of funds as defined in article 11(b)(ii) of 4AMLD is considered as commensurate to the risk (i.e. EUR1 000). In addition, Member States should provide guidance on the definition of occasional transactions providing for criteria ensuring that the CDD rules applicable to business relationship are not circumvented.

Illegal transfers of funds - Hawala

Product
Illegal/informal transfer of funds through hawala

General description
Hawala predates traditional or western banking and is one of the informal funds transfer (IFT) systems that are in use in many regions for transferring funds, both domestically and internationally. These IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. Hawala payments are informal funds transfers that are made without the involvement of authorised financial institutions. In principle the money does not physically move from the payer to the payee, but is, as is also often the case in money remittances, done through an offsetting of balances between the hawaladar of the payer and the hawaladar of the payee. Contrary to regulated remittance systems, IFT is based on a network of key players (Hawaladars) tied by trust (due to specific geographic regions, families, tribes, ethnic communities, nationalities, commercial activity, etc) and who compensate each other by net settlement over a long period of time using banking channels, trade or cash. This means that, contrary to all other remittance systems, no funds are transferred for each and every transaction, but there is a net settlement. They use a local cash pool with money that was already in the system to pay the beneficiary. After a set period of time (usually after 2-3 months) only the net amount is settled. Hawaladars aggregate months of funds received through individual remitters and then perform the settlement. To illustrate this modus operandi, a hawaladar from country A (HA) receives funds in one currency from the payer and, in return, gives the payer a code for authentication purposes. He then instructs his country B correspondent (HB) to deliver an equivalent amount in the local currency to a designated beneficiary, who needs to disclose the code to receive the funds. After the remittance, HA has a liability to HB, and the settlement of their positions is made by various means, either financial or goods and services. Hawala is often used by migrant workers to transfer money to overseas relatives in developing countries without the high costs of currency exchange and with lower handling costs compared to a regular remittance. As Hawala does not take place between licenced and supervised financial entities, the engagements between all parties are based on connections and trust. The cost effectiveness, the swifter transmission of amounts as compared to classical remittances, often requiring correspondent banking, and the lack of a paper trail, has made this type of transfers popular. Not being regulated, hawaladars do not feel bound by formal exchange rates, thereby allowing them to offer lower exchange rates than the regulated counterparties. Hawaladars can engage in foreign exchange speculation by exploiting naturally occurring fluctuations in the demand for different currencies. This enables them to make a profit from hawala transactions. There is no reliable quantifiable data on the size of Hawala in the EU or globally, as the entities are not supervised and their money flows are not processed through authorised payment systems and therefore not systematically monitored (although traces may exist when compensation take place). There is limited/no information to be able to assess the size

of the problem in the EU – and to assess to what extent hawala services exist in the EU.

Hawala payments show a large resemblance to remittances, except that the transfers take place between natural persons. As the service that they provide can be equated to remittance, the hawaladars, when operating from within the EU, should therefore be authorised under the Payment Services Directive to do so.

There are known risks to the use of Hawala payments. Reports from the US Treasury indicate that Hawala is known to be used for hiding cash flows that normally would be subject to VAT or other taxation rules on their other (import/export) business in the country where the Hawala dealer is operating. The manipulation of invoices is a very common means of settling accounts after the transactions have been made. A Hawala dealer manipulates the invoices on products that are shipped to the Hawala dealer abroad (under-invoicing). By doing so, it settles its debt following from the Hawala business and avoids tax payments. Vice-versa, by "over-invoicing" imported products, the Hawala dealer can arrange to be paid by the other Hawala dealer abroad for the payment that it has done to a beneficiary at the request of the Hawala dealer abroad.

The anonymity and minimal documentation of Hawala transactions has made it vulnerable to be used for illegal activities or money laundering purposes. There is a consensus that, in the wake of heightened international efforts to combat money laundering and terrorist financing, more should be done to keep an eye on IFT systems to avoid their misuse by illicit groups. This issue was lately discussed in the context of G7 FMs&CBGs Meeting in Washington D.C. on 20 April 2017.

Description of the risk scenario

Perpetrators are using hawala and informal transfers of funds to channel funds for ML/TF purposes. Perpetrators are attracted since hawala and similar illegal services do not ensure traceability of transactions / reporting of suspicious transactions. The system works via a system of net settlement over a long period of time using banking channels, trade or cash. Contrary to all other remittance systems, funds are not transferred for each and every transaction; Hawala uses net settlement. Also, within the Hawala network unique techniques are used:

-Bilateral settlement, the “reverse hawala” between two Hawaladars.

-Multilateral settlement, “triangular”, “quadrangular” or other between several Hawaladars part of the same network.

-Value settlement through trade transactions, usually applying TBML techniques (shipment of the equivalent value through trade transactions, such as merchandise or other commodities such as paying a debt or invoice of same value that they owe, over or under invoicing, double invoicing, Black Market Peso Exchange, etc.).

-Settlement through cash via cross-border cash couriers, banking and MSB channels.

Particular Hawala networks are created to serve exclusively criminal needs, by placing and layering criminal money and paying the equivalent value on demand elsewhere in the world. They are known to use the techniques described above. In addition to protect themselves they use these particular measures:

- Quick cash pick ups.

- Authentication via Token.

- Placement via cuckoo smurfing.

All these techniques are unique to the Hawala system and are all known red flag indicators of Hawala activities for EU LEAs.

Such particular Hawala networks – the Criminal Hawala, also follows a particular structure, composed of:

- Controllers or money Brokers – makes the deal with the OCGs for the collection of dirty cash and for delivery of its value on a chosen destination.
- Co-ordinators - an intermediary working for the Controller and managing different Collectors.
- Collectors – collects dirty cash from criminals and disposes of it.
- Transmitter - receives and dispatches the money obtained by the Collector (usually an MSB operator).

Threat

N/A

Those IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. The size of the problem is not easily identified due to the lack of information.

According to Europol information, it seems associated to certain businesses (Travel agencies, pawn shops, mobile phones and, SIM cards sales, top-up of mobile cards, grocery stores, import/export business and various neighbourhood type of businesses as nail salons, hairdressers, beauty salons, flower shops) of certain ethnic communities (India, Afghanistan, Pakistan, Iran, United Arab Emirates, Somalia and China) that are extremely common in the EU. Europol is also aware of several multi-million EUR on-going money laundering investigations focusing on criminal Hawala.

Since there are no direct money/value flows between sender and receiver that LEAs can track or trace, tracing the money/value flow in a Hawala network is virtually impossible. Even if ledgers are seized, it is not possible to trace money/value flow since those ledgers are usually encrypted and are increasingly located on cloud servers located in non-cooperative jurisdictions. This opacity makes it attractive for perpetrators.

Vulnerability

N/A

Those IFT are considered as unregulated payment services under EU law; hence they are illegal within the EU. There is no specific vulnerability assessment for illegal services in the context of the SNRA

Mitigating measures

- The Commission services together with Europol and the ESAs will carry out an analysis of Informal Funds Transfer/Hawala in order to define the size of the problem and suitable measures to reduce the threat posed by these illegal activities.

Payment services

Product

Payment services

Sector

Credit and financial sector

General description of the sector and related product/activity concerned

Payment services regulated by the Payment Services Directive (2007/64/EC) cover a wide variety of services. They range from cash deposits and withdrawals from bank and payment accounts (cash deposits are addressed in a separate fiche), money remittance (see separate fiche as well), the execution of payment transactions such as credit transfers, direct debit transactions and payments with credit and debit cards. A 'payment transaction' is defined as an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

Furthermore, PSD covers the issuing of payment instruments, such as debit and credit cards and the acquiring of payment transactions on the payee's side.
PSD does not regulate all payments. Payments in cash or paper cheque payments are not covered, and neither are payments sent through an intermediary of a telecom IT or network operator. They may however be regulated at national level by the Member States.
Recently, the PSD has been revised. The revised PSD, commonly referred to as PSD2, entered into force on 13 January 2016. With a transitional period of two years for Member States to implement the provisions, PSD2 will become applicable on 13 January 2018.
PSD2 will cover additional payment services which have emerged during the past years in the slipstream of the digitalization of the services. These services are referred to as payment initiation services (PIS). PIS allow consumers to pay for their online purchases by a simple credit transfer instead of a credit card payment (around 60% of the EU population does not have a credit card). The service provider can check if there are sufficient funds on the consumer's account balance to make the payment. It informs the merchant immediately that the payment order has been sent to the payer's bank, which will allow the web merchant to already ship the goods or render the service before the amount is booked on his account. PSD2 will cover these new payments addressing issues which may arise with respect to confidentiality, liability or security of such transactions.

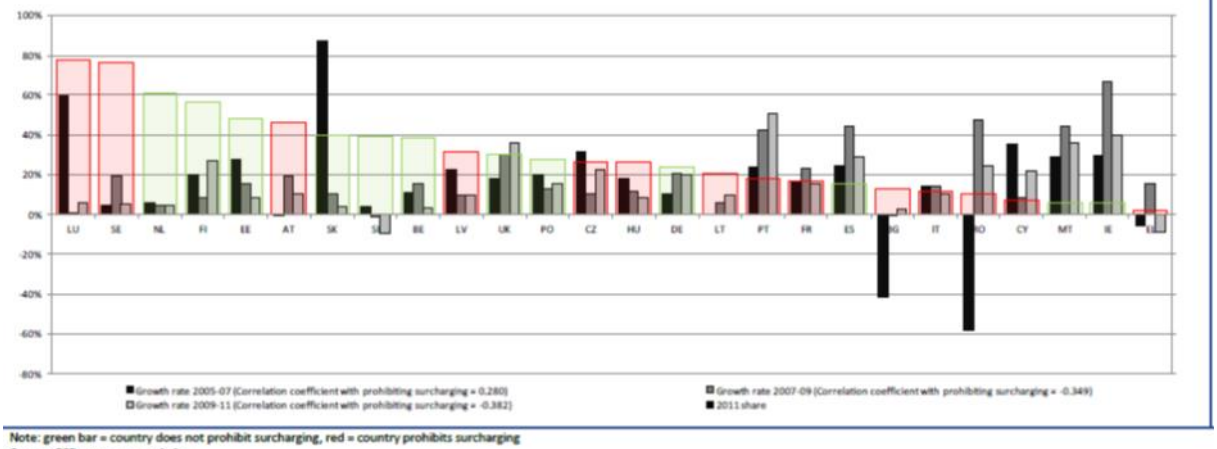
The large majority of payments are done electronically. The total number of non-cash payments in the EU increased by 2.8% to 103.2 billion in 2014 compared to the previous year:
- payments with credit and debit cards accounted for 46% of all transactions,
- credit transfers accounted for 26% and direct debits for 21%,
- the number of direct debits in the EU decreased in 2014 by 6.6% to 21.9 billion,
- the number of credit transfers remained unchanged at 27.0 billion,

The number of cards with a payment function in the EU increased in 2014 by 0.9% to 766 million, with a total EU population of 509 million, this represented around 1.5 payment cards per EU inhabitant. The number of card transactions rose by 8.8% to 47.5 billion, with a total value of EUR 2.4 trillion. This corresponds to an average value of around EUR 50 per card transaction (Source: ECB, more information on the relative importance of each of the

main payment services across EU countries in 2014 can be found in annex 1).

The tables below show the level of the share of card usage in total card and cash usage in 2011 (large bars in green and red) and the growth in the share of card usage in total card and cash usage over the three periods). Most of the EU countries saw a significant increase in the card use since 2011 until 2014, with a few exceptions of decreased usage in Portugal, Ireland, Luxembourg, Malta and Austria.

Figure 33:The share of transactions accounted for by cards when considering those made by cash, cheque or cards



Note: green bar = country does not prohibit surcharging, red = country prohibits surcharging

Source: ECB payments statistics

Retail payment systems

Retail payment systems in the EU have payments that are made by the public, with a relatively low value, a high volume and limited time-criticality. In 2014, 42 retail payment systems existed within the EU as a whole. During the year, almost 50 billion transactions were processed by those systems with an amount of EUR 38.3 trillion. 23 of these systems were located in the euro area, where they processed nearly 37 billion transactions in 2014 (i.e. 74% of the EU total) with a value amounting to EUR 27.2 trillion (i.e. 71% of the EU total).

Large-value payment systems

Large-value payment systems (LVPSs) are designed primarily to process urgent or large-value interbank payments, but some of them also settle a large number of retail payments. During 2014, 14 systems settled 749 million payments with a total value of EUR 682 trillion in the EU. The two main LVPSs in the euro area (TARGET2 and EURO1/STEP1) settled 145 million transactions amounting to EUR 541 trillion in 2014, i.e. 79% of the total value.

Payment service providers

Within the EU, not only credit institutions are allowed to provide payment services. In addition, electronic money institutions, post giro institutions and regional or local authorities where they do not act as public authorities can do so. In addition, with the adoption of PSD in 2007, a new entity has been introduced, the so-called payment institutions, which can only provide payment services and are not allowed to take deposits or issue e-money.

The introduction of payment institutions has increased competition in the payments market since 2009.

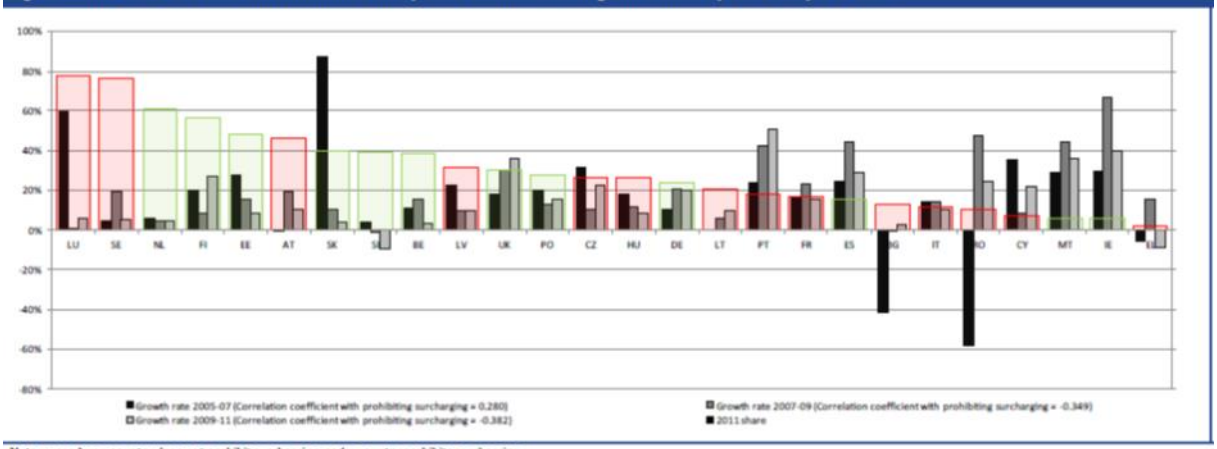
The large majority of payments are done electronically. The total number of non-cash payments in the EU, increased by 2.8% to 103.2 billion in 2014 compared with the previous year:

- card payments accounted for 46% of all transactions,
- credit transfers accounted for 26% and direct debits for 21%,
- the number of direct debits in the EU decreased in 2014 by 6.6% to 21.9 billion,
- the number of credit transfers remained unchanged at 27.0 billion,

The number of cards with a payment function in the EU increased in 2014 by 0.9% to 766 million, with a total EU population of 509 million, this represented around 1.5 payment cards per EU inhabitant. The number of card transactions rose by 8.8% to 47.5 billion, with a total value of EUR 2.4 trillion. This corresponds to an average value of around EUR 50 per card transaction (Source: ECB, more information on the relative importance of each of the main payment services across EU countries in 2014 can be found in annex 1).

The tables below show the level of the share of card usage in total card and cash usage in 2011 (large bars in green and red) and the growth in the share of card usage in total card and cash usage over the three periods). Most of the EU countries had a significant increase in the card use since 2011 until 2014, with few exceptions of decreased usage in Portugal, Ireland, Luxembourg, Malta and Austria.

Figure 33:The share of transactions accounted for by cards when considering those made by cash, cheque or cards



Note: green bar = country does not prohibit surcharging, red = country prohibits surcharging

Source: ECB payments statistics

The following table shows the ECB statistics of institutions providing payment services:

Table 3: ECB payments statistics - number of institutions offering payment services[1] and value and volume of transactions in 2011

Country	Total number of institutions providing payment services to non-MFIs	Total value of transactions (EUR trillions)		Total number of transactions		Average value in EUR
		EUR trillions	Percentage of total	millions	Percentage of total	
Austria	767	2.90	1.2%	2,363.10	2.6%	1,226.67
Belgium	110	4.07	1.7%	2,501.31	2.8%	1,626.56
Bulgaria	40	0.14	0.1%	101.97	0.1%	1,328.56
Cyprus	151	0.63	0.3%	93.70	0.1%	6,764.97
Czech Republic	60	1.75	0.7%	979.75	1.1%	1,791.20
Denmark	162	0.77	0.3%	1,695.38	1.9%	452.61
Estonia	45	0.16	0.1%	313.59	0.3%	516.50
Finland	344	4.46	1.9%	2,183.36	2.4%	2,044.97
France	662	28.42	11.8%	17,538.26	19.4%	1,620.71
Germany	1942	67.99	28.3%	17,775.92	19.6%	3,824.60
Greece	59	1.25	0.5%	189.23	0.2%	6,582.99
Hungary	194	1.67	0.7%	852.14	0.9%	1,963.59
Ireland	483	0.69	0.3%	682.75	0.8%	1,016.20
Italy	797	10.05	4.2%	4,159.58	4.6%	2,415.11
Latvia	28	0.42	0.2%	238.58	0.3%	1,773.77
Lithuania	114	0.22	0.1%	275.84	0.3%	809.57
Luxembourg	147	1.13	0.5%	927.84	1.0%	1,217.16
Malta	34	0.13	0.1%	31.83	0.0%	4,161.67
Netherlands	306	6.87	2.9%	5,647.85	6.2%	1,216.70
Poland	1083	7.93	3.3%	2,674.51	3.0%	2,965.47
Portugal	269	1.77	0.7%	1,791.74	2.0%	987.61
Romania	51	1.43	0.6%	322.20	0.4%	4,436.82
Slovakia	35	0.88	0.4%	503.97	0.6%	1,752.00
Slovenia	35	0.34	0.1%	339.75	0.4%	1,004.78
Spain	337	11.92	5.0%	5,535.92	6.1%	2,152.75
Sweden	199	1.54	0.6%	3,071.23	3.4%	502.76
United Kingdom	375	80.69	33.6%	17,794.86	19.6%	4,534.38
EU Total	8829	240.24	100.0%	90,586.14	100.0%	2,652.06

Note: The institutions covered by the ECB statistics reported in the table above include all credit institutions of the EU27 but only a few of the existing payment institutions and e-money institutions

Source: European Central Bank, Payment Statistics, data as of September 2012

The majority of payment service providers still consist of credit institutions and the like.

As for the smaller players, EU wide (status 2012), there were 568 authorised payment institutions (APIs), 2,203 small payment institutions (SPSPs, payment institutions that are only allowed to provide payment service in the country where they have obtained a licence) and 71 e-money institutions. The distribution of payment institutions (APIs and SPSPs) is highly concentrated, in each case a few countries accounting for the vast majority of such institutions in the EEA. The UK accounts for 39.4% of all APIs in the EEA, and the UK together with Spain (8.1%), Italy (7.9%), Germany (6.5%), Netherlands (4.9%) and Sweden

(4.3%) account for 71% of all APIs in the EEA. As for the SPSPs, 44.8% were registered in Poland, and 43.6% were registered in the UK. The UK also accounted for 42.2% of all e-money institutions in the EEA.

Description of the risk scenario

Perpetrators are using the banking and financial system to channel their funds through bank accounts, wire credit and debit transfers, (peer-to-peer) mobile payments and Internet-Based Payment Services

Threat

Terrorist financing

The assessment of the TF threat related to payment services shows that account-based transactions are used by terrorists to store and transfer funds and to pay for the services or products needed to carry out their operations, in particular when processed through the internet. According to research on the financing of European jihadist terrorist cells, the formal banking system is one of the six methods most commonly used by terrorist groups. The majority of terrorist cells located in Europe have derived some income from legal sources – usually received through the formal banking system – and use bank accounts and credit cards both for their everyday economic activities and for attack-related expenses. Due to the account based elements terrorist groups' intent to rely on this risk scenario is more limited. However their capability to use it is quite high. Payment services allow cross-border transactions that may rely on different mechanisms of identification (depending on national legislations) that may lead the terrorists to use false identity. Thus, LEAs cannot track the originator or beneficiary of the transaction. It requires specific skills but, according to LEAs, these skills are commonly widespread within terrorist groups and do not constitute an obstacle (mobile/internet payments quite easy). The amounts concerned seem to remain, nevertheless, quite limited.

Conclusions: terrorist groups use payment services to finance terrorist activities. They rely on IT skills to circumvent identification requirements and do not need specific knowledge to access this channel which is rather attractive and secure. The amounts concerned remain nevertheless quite limited. In that context, the level of TF threat related to payment services is considered as significant (level 3).

Money laundering

The assessment of the ML threat related to payment services has been considered as presenting similarities with deposits on account /retail banking. This risk scenario concerns both placing funds and withdrawing funds (i.e. deposits on account and use of this account). It is frequently used by criminals but also by relatives/close associates and this extends the scope of the intent and capability analysis. The source of the funds used in payment services is coming from non-legitimate origin. It requires a bit of planning and knowledge of how banking systems work.

Conclusions: criminal group organisations use rather frequently this modus operandi which is easily accessible, although it requires some knowledge and planning capabilities to ensure that origin of funds is hidden. In that context, the level of ML threat related to payment services is considered as significant/very significant (level 3/4)

Vulnerability
Terrorist financing The assessment of the TF vulnerability related to payment services presents some commonalities with the assessment of TF vulnerability concerning retail payment services. **(a) risk exposure:** It is inherently high due to the characteristics of payment services. They involve very significant volumes of products and services. Although they are generally not anonymous (as they are linked to an identified account), they may interplay with very significant volumes of higher risk customers or countries, including cross-border movements of funds. They also interact with new payment methods (mobile/internet) which may increase the level of risk exposure because it implies, by definition, a non-face-to-face business relationship. **(b) risk awareness** The risk awareness is quite good due to the fact that the sector has put in place guidance to detect the relevant red flags on TF. This is confirmed by a good level of reporting, as the sector seems to have adequate tools to detect these risks. However, CDD and risk indicators are not always sufficient to detect a link to terrorist activities due to the legitimate origin of the funds. Competent authorities are also well aware about the vulnerabilities of the sector (see Egmont group project on ISIL) and are proactively engaged with the sector. **(c) legal framework and controls** Payment services are included in the AML/CFT legal framework at EU level. This framework is in place for many years and controls are considered globally as efficient. As far as the legal framework is concerned, it covers equally bank and payment institutions. Controls in place are nevertheless less efficient when dealing with payment institutions. New risks and opportunities may emerge with FinTech/RegTech. **Conclusions: although the risk exposure may be considered as quite high (significant level of transactions), the sector shows a good level of awareness to the risk vulnerability and is able to put in place the relevant red flags. The legal framework and controls are the basis of a good level of reporting. In that context, the level of TF vulnerability related to payment services is considered as moderately significant. (level 2)**
Money laundering The assessment of the ML vulnerability related to payment services presents some commonalities with the assessment of ML vulnerability related to retail services. **(a) risk exposure:** It is inherently high due to the characteristics of payment services. They involve very significant volumes of products and services. Although they are generally not anonymous (as they are linked to an identified account), they may interplay with very significant volumes of higher risk customers or countries, including cross-border movements of funds. They also interact with new payment methods (mobile/internet) which may increase the level of risk exposure because it implies, by definition, a non-face-to-face business relationship.

(b) risk exposure:
Competent authorities have noticed some discrepancies between banking and payment institutions, the latter being less aware of ML risks. Agents of payment institutions have, most of the time, an insufficient knowledge of AML rules, leading to a low level of CDD and weak controls (in particular due to lower human resources). The insufficient monitoring is present both at the opening of the payment account (entry point) and at the processing of the transaction.
(c) legal framework and controls:
Payment services are included in the AML/CFT legal framework at EU level. As far as the legal framework is concerned, it covers equally bank and payment institutions. The reliance on account-based transactions implies that the legal framework applies commonly to bank and not banks entities. This framework is in place for many years and controls are considered globally as efficient. Controls in place are nevertheless less efficient when dealing with payment institutions. New risks and opportunities may emerge with FinTech/RegTech.

Conclusions: the risk exposure and the risk awareness of the sector are quite similar to what happens in the retails services sector. As far as the legal framework is concerned, it covers equally bank and payment institutions. Controls in place are nevertheless less efficient when dealing with payment institutions. In that context, the level of ML vulnerability related to payment services is considered as moderately significant (level 2).

Mitigating measures

- The 4AMLD will reinforce CDD measures with regard to occasional transactions for funds transfer (threshold of EUR 1000 applicable for transfers of funds – which triggers CDD obligations).

For credit institutions:

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):
  (i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include interconnection of beneficial ownership registers at EU level.
  (ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements

- The Commission will launch further analysis in order to identify risks and opportunities on FinTech/RegTech. The Commission FinTech Task Force will assess technological developments, technology enabled services and business models, will determine whether existing rules and policies are fit for purpose and will identify options and proposals to harness opportunities or address possible risks.

- The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed

- Updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in credit institutions should be

provided by the ESAs. The Commission services will further analyse whether those guidelines allow the position of the AML/CFT – compliance officer to be sufficiently reinforced.

For financial institutions

- Member States should ensure that supervisors conduct a number of on-site inspections commensurate to the level of ML/TF risks identified. Those inspections should include a review of training carried out by agents of obliged entities.
- Member States' supervisors should carry out a thematic inspection in the MVTS sector within 2 years, except for those that carried out recently such thematic inspections. The results of the thematic inspections should be communicated to the Commission.
- In addition, competent authorities should provide further risk awareness and risk indicators relating to terrorist financing to the MVTS sector. The obliged entities should provide mandatory training to agents to ensure that they are aware about their AML/CFT obligations and how to detect suspicious transactions.
- Pending the application of 4AMLD, Member States should define a threshold below EUR 15 000 triggering CDD obligations in case of occasional transactions, which is commensurate to the AML/CFT risk identified at national level. A threshold similar to the one for occasional transactions for transfers of funds as defined in article 11(b)(ii) of 4AMLD is considered as commensurate to the risk (i.e. EUR 1000). In addition, Member States should provide guidance on the definition of occasional transactions providing for criteria ensuring that the CDD rules applicable to business relationship are not circumvented.

Virtual currencies

Product

Virtual currencies

Sector

Virtual currencies providers

General description of the sector and related product/activity concerned

Definitions

"Virtual currencies" means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically.

Various stakeholders are involved in the virtual currency market with the main ones being:

- **User** : 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.

- **Miners:** in decentralised VC schemes, miners deliberately solve 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).

There 2 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 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 fiat currency,

fiat currency 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.

The VC market in the EU

Official data regarding the market is hard to reach. Based on various websites tracking volumes and prices of exchanges or conducting research, the following estimations could be given. Market players tend 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)[10] – 7.4 million in Q4 2014
VC wallets in the EU	About 3 million
VC users worldwide[11]	From 1 to 4 million
VC users in the EU	About 500.000
VC miners worldwide	100.000[12]
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[13]	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	EUR7 billion

Description of the risk scenario

ML: Perpetrators use virtual currency systems traded on the internet to transfer funds or purchase goods anonymously (cash funding or third-party funding through virtual exchangers).

TF: Virtual currency systems can be traded on the internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding or purchase (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

[10] http://www.coindesk.com/state-of-bitcoin-blockchain-2016/ Slide 8
[11] At least one transaction per month
[12] http://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/
[13] http://coinatmradar.com/ (consulted 4.2.2016)

Threat

Terrorist financing

The assessment of the TF threat related to virtual currencies shows that terrorist groups may have some interest in using VCs to finance terrorist activities. A limited but increasing number of cases related to TF through VCs have been reported. Egmont group has identified virtual currencies as a tool by terrorist groups and terrorist groups are known to have given instructions on the internet (including via twitter) on how to use VCs. However, the technology is quite recent and in any case requires some knowledge and technical expertise which has a dissuasive effect on terrorist groups. The reliance on virtual currencies to fund terrorist activities has some costs and is not necessarily attractive.

Conclusions: LEAs have gathered some information according to which terrorist groups may use virtual currencies to finance terrorist activities. However, the use of virtual currencies requires technical expertise which makes it less attractive. Consequently, the level of TF threat related to virtual currencies is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to virtual currencies shows that organised crime organisations may use virtual currencies to have access to "clean cash" (both cash in/out). When used, virtual currencies allow organised crime groups to access cash anonymously and hide the transaction trail. They may acquire private keys of the e-wallets or obtain some cash from ATM. However, cases are quite rare at this stage and few investigations have been undertaken concerning this risk scenario. One of the reasons is that the reliance on virtual currencies to launder proceeds of crime requires some technical expertise. According to LEAs, the amounts of money laundered via virtual currencies are quite low, which tends to demonstrate that criminals' intent to use them is rather limited because this modus operandi is not considered as attractive enough (in particular because of the volatility of the virtual currencies' market). From a technical point, virtual currencies present some commonalities with e-money but the IT expertise at stake for virtual currencies means that organised crime would have lower capability to use them than e-money which is more widely accepted.

Conclusions: few investigations have been conducted on virtual currencies which seem to be rarely used by criminal organisations. While they may have a high intent to use due to VCs characteristics (anonymity in particular), the level of capability is lower due to high technology required. Consequently, the level of ML threat related to virtual currencies is considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to virtual currencies providers shall take into account the fact that, currently, virtual currencies are not regulated in the EU and that the risks of being misused for TF purposes are only just emerging.

a) risk exposure:

When used anonymously, virtual currencies allow conducting transactions speedily and without having to disclose the identity of the "owner". By nature, given that they are provided through the internet, the cross-border element is the most prevailing one, increasing the risk to interact with high risk areas or high risk customers that cannot be identified. It is nevertheless important to mention that being currently a developing technology requiring IT

skills and expertise, virtual currencies are not necessarily easy to use and the number of transactions is still quite low.

b) risk awareness:

This component of the TF vulnerability is difficult to assess in a comprehensive manner due to the fact that virtual currencies providers are not regulated as obliged entities at European level at this stage. Evidently, at the moment there is no reporting from VCs providers which does not mean that the sector is not equipped to do so. Nevertheless, competent authorities and FIUs have noticed in their exchanges with the sector that, at this stage, the level of awareness to TF risk is rather low, even if the sector is asking for the adoption of an appropriate AML/CFT legal framework. The sector is not well organised yet and it is difficult to find adequate tools to provide relevant information to the sector in order to increase the level of awareness;

c) legal framework and controls:

The lack of a legal framework is the most important element of vulnerability. In the current situation, VCs providers cannot be monitored and supervised. There are no common rules in the EU to ensure that VCs providers apply AML/CFT requirements. The international cooperation is non-existent. New risks and opportunities may emerge with FinTech/RegTech.

Conclusions: the most important element of vulnerability for virtual currencies providers is the fact that there are not regulated in the EU. They cannot be properly monitored and they cannot report suspicious transactions to FIU. The inherent risk exposure is also very high due to the features of the virtual currencies (internet, cross-border and anonymity). Finally, the sector is currently not organised well enough to receive guidance or relevant information on AML/CFT requirements. Consequently, the level of TF vulnerabilities related to virtual currencies is considered as significant/very significant (level 3/4).

Money laundering

The assessment of the ML vulnerability related to virtual currencies providers starts from the same caveat as for TF. They are not regulated in the EU and there is little evidence of VCs being misused for ML purposes. However, this does not impede an assessment of the potential vulnerabilities of this risk scenario. There are still few investigations leading to prosecutions but the risk exists and can be analysed.

a) risk exposure:

Similarly to TF, when used anonymously, virtual currencies allow conducting transactions speedily and without having to disclose the identity of the "owner". By nature, given that they are provided through the internet, the cross-border element is the most prevailing one, increasing the risk to interact with high risk areas or high risk customers (darknet) that cannot be identified. At the stage of the conversion, the use of cash also becomes a new element of vulnerability. The delivery channels are decentralised which increases the risk exposure as well (in particular, ATM offer virtual currencies withdrawal or conversion process). It is nevertheless important to mention that being currently a developing technology requiring IT skills and expertise, virtual currencies are not necessarily easy to use and the number of transactions is still quite low.

b) risk awareness:

Given the emerging technology concerned, the level of risk awareness from the sector is not granted. Nevertheless, the sector is more and more in need of a legal framework in order for the AML/CFT requirements to be applicable to virtual currencies. FIUs cannot detect and analyse the risk on the basis of the sole blockchain. They cannot identify the amount of funds stored in the wallet and the origin/beneficiary of the funds is also impossible to identify.

c) legal framework and controls:

Again, similarly to TF, the lack of legal framework is the most important element of vulnerability. In the current situation, VCs providers cannot be monitored and supervised. There are no controls in place and no common rules in the EU to ensure that VCs providers apply AML/CFT requirements. The international cooperation is non-existent. New risks and opportunities may emerge with FinTech/RegTech.

Conclusions: the assessment of ML vulnerability presents commonalities with TF. The most important element of vulnerability for virtual currencies providers is the fact that there are not regulated in the EU. They cannot be properly monitored and they cannot report suspicious transactions to FIUs. The inherent risk exposure is also very high due to the features of the virtual currencies (internet, cross-border and anonymity). Finally, the sector is currently not organised well enough to receive guidance or relevant information on AML/CFT requirements. In that context, the level of TF vulnerabilities related to virtual currencies is considered as significant/very significant (level 3/4).

Mitigating measures

- The Commission proposed in its proposal for amending Directive (UE) 2015/849 that virtual currency exchange platforms as well as custodian wallet providers are added to the list of obliged entities under 4AMLD.
- The Commission would issue a report to be accompanied, if necessary, by proposals, including, where appropriate, with respect to virtual currencies, empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to FIUs, as well as self-declaration forms for the use of virtual currency users.
- The Commission will continue to monitor in the context of the SNRA the risks posed by FinTech/RegTech, crypto-to-crypto currency exchanges, and use of virtual currencies for purchasing of high value goods.

Business loans

Product

Credit loan

Sector

Credit and financial sector (including insurance companies)

Description of the risk scenario

Perpetrators repay business loans with criminal funds (including use of the credit card for repayments in order to legitimise sources of funds). Loans provide legitimacy to criminal funds.

Threat

Terrorist financing

The assessment of the TF threat related to business loans shows that there few cases where terrorist organisations have used this scenario to collect funds. Business loans are not easily accessible to terrorist organisations because they do not fulfil the conditions to subscribe to this kind of products (level of salary too low, origins of funds coming from social benefits). There are also few cases where sanctioned entities (listed organisations) may try to use business loans to finance terrorist activities through shell companies. However, it requires a sophisticated level of expertise and knowledge.

Conclusions: considering that there is little evidence that criminals used/have the intention to use this modus operandi, the level of TF threat related to business loans is considered as lowly significant (level 1).

Money laundering

The assessment of the ML threat related to business loans shows that there are few indicators that criminals have the intention to exploit this risk scenario which is perceived as unattractive. Fake loans are most of the time part of fraud schemes (e.g. 2 companies subscribe to a fake loan and use a bank to process the transfer of funds) but are not necessarily use to launder proceeds of crime.

Conclusions: considering that there is little evidence that criminals used/have the intention to use this modus operandi, the level of ML threat related to business loans is considered as lowly significant (level 1).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to business loans has been considered in conjunction with ML schemes related to business loans. In that context, the TF vulnerability does not benefit from a separate assessment.

Conclusions: the level of ML vulnerability is considered as lowly significant (level 1).

Money laundering

The assessment of the ML vulnerability related to business loans shows that:

(a) the risk exposure:
It is quite limited due to the nature of the product itself which implies high value loans that are not granted as easily as consumer credit. Business loans are not particularly exposed to high risk customers or high risk areas, and they are granted generally via secured channels.

(b) risk awareness:
Financial institutions appear to be sufficiently aware of the risk of fraud that may arise in relation to business loans. They pay particular attention to the risk of forged documentation or fake identity, as they also need to be sure that they can recover the funds granted.

(c) legal framework:
Business loans are covered by the AML/CFT framework at EU level. Controls in place are considered as consistent with the volume of transactions concerned.

Conclusions: the level of ML vulnerability is considered as lowly significant (level 1).

Mitigating measures

No further proposal is made at this stage

Consumer credit and low value loans

Product

Credit loan

Sector

Credit and financial sector

Description of the risk scenario

Terrorists/organised crime groups use "payday", consumer credit or student loans (short-term, low value but high interest) to fund plots. Loans are given for relatively low amounts allowing the access to funds, the sources for which are untraceable as long as the money is not transferred.

Terrorists/organised crime groups use cash withdrawals with credit cards: criminals withdraw cash with their own credit cards on an ATM, generating a negative balance on their accounts. They disappear with the funds without any intention to reimburse this "forced" credit.

Threat

Terrorist financing

The assessment of the TF threat related to consumer credit and low value loans shows that this modus operandi is used by terrorist groups to finance travels of foreign terrorist fighters to high risk third countries. The most widespread product is the consumer credit. Low value loans are perceived as rather attractive and as not requiring necessarily a high level of expertise or planning. Nevertheless, and depending on national legislation, the expertise required may vary where specific documentation is needed. It implies that terrorist groups have the capacities to forge some documents.

Conclusions: consumer credit and low value loans are attractive for terrorist groups who have used/are using this modus operandi quite frequently. Certain legislative frameworks may impose specific conditions to acquire consumer credit or low value loans but this does not seem to constitute an obstacle for terrorist organisations. In that context, the level of TF related to low value loans is considered as significant (level 3).

Money laundering

The assessment of the ML threat related to low value loans has not been considered as particularly relevant. In that context, the ML threat is not part of the assessment.

Conclusions: non relevant

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to consumer credits/ low value loans shows that

(a) risk exposure:

From its characteristics, a consumer credit/low value loan does not expose the sector to high vulnerabilities. In general, low amounts are at stake (EUR 1000 is the most common amount), with no involvement of high risk customers or high risk countries. These products are generally granted to students or vulnerable people submitted to specific controls and checks by financial institutions.

(b) risk awareness:
This assumed low risk exposure is nevertheless overcome by the fact that, because of the small amounts, the sector is less aware of the TF risks. In addition, similarly to what has been analysed for the business loans, the risk awareness seems more oriented towards risks of fraud than risk of TF. Hence, the sector does not necessarily trigger any TF red flags. IT systems in place are not necessarily equipped to detect forged documents. Competent authorities consider, in addition, that the level of vulnerability depends on the structure which grants the loan: investigations have shown that consumer credit/low value loans funds are now proposed by phone companies which are not supervised for AML/CFT requirements. FIUs have also noticed that STRs are sometimes filed too late (e.g. when a large amount is withdrawn in one go) which makes furthering the investigations almost impossible as the presumed terrorist is already gone.

(c) legal framework and controls:
Consumer credits/low value loans are covered by the AML/CFT framework at EU level. However, national legislations differ a lot from one Member State to another, as far as the request for documents is concerned. Some Member States require specific documents while others do not. When the loan is granted by a bank, the risks are not necessarily completely mitigated because the funds from loans deposited on a bank account may be withdrawn via ATM with no control. New risks and opportunities may emerge with FinTech/RegTech.

Conclusions: while the volume of transactions and amounts at stake limit the risk exposure of the sector, it appears that the sector is not necessarily aware of the TF risks related to consumer credit/low value loans. The differences between national legislative frameworks show that the capacity of competent authorities and FIUs to detect suspicious transactions is limited, especially when loans are granted by non-financial entities. In that context, the level of TF vulnerability related to low value loans is considered as significant (level 3).

Money laundering

The assessment of the ML vulnerability related to low value loans has not been considered as particularly relevant. In that context, the ML threat is not part of the assessment.

Conclusions: non relevant

Mitigating measure

Competent authorities should put in place systems to allow obliged entities to detect forged documents.

Mortgage credit and high value asset-backed credits

Product

Mortgage credit

Sector

Credit and financial sector

Description of the risk scenario

In the case of money laundering, perpetrators disguise and invest proceeds of crime by way of real estate investment. Proceeds of crime are used for deposit, repayments and early repayment of asset.

In the case of terrorist financing, perpetrators use high value assets backed credit/mortgage loans (medium/long-term, high value with low interest) to fund plots. Loans are subscribed for relative high amounts to access funds which are untraceable as long as the money is not transferred.

Threat

Terrorist financing

The assessment of the TF threat related to mortgage credit shows that this modus operandi is really difficult to use and to access by terrorist groups. There are few cases where terrorist organisations have used this scenario to collect funds. In addition, they are not attractive because they do not correspond to the needs of terrorist organisations. It requires sophisticated knowledge and technical expertise to be able to produce complex documentations. In addition, it is not attractive because the inherent nature of mortgage credit is to give access to funds to a third party, so it does not allow an easy and speedy access to funds by terrorist organisations, unless complicity has been built with this third party.

Conclusions: mortgage credit requires a high level of knowledge and expertise to understand the product and to provide the relevant documentation (forged documents). It is not attractive due to the fact that it implies the complicity of a third party, beneficiary of the funds. In that context, the level of TF threat related to mortgage credit is considered as lowly significant (level 1).

Money laundering

The assessment of the ML threat related to mortgage credit shows that organised crime organisations have frequently used this modus operandi. They are well equipped to provide false documentation and the structure of the mortgage (third party) assists in hiding the real beneficiary of the funds. It constitutes an easy way to commit fraud because it may lead to the ownership of several pieces of properties to hide the volume of assets.

Conclusions: in the ML context, mortgage credit is a vehicle favoured by criminal organisations. It allows hiding the volume of assets and the beneficial ownership. It requires a moderate level of expertise. Consequently, the level of ML threat related to mortgage credit is considered as significant (level 3).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to mortgage credit shows that this product is not vulnerable to TF risks because few or even no cases were found by LEAs. The risk awareness of the sector is quite low but this does not mean that the risk is unknown, but that it is unlikely and that red flags are adequate in case of suspicion of fraud.

Conclusions: moderately significant (level 2)

Money laundering

The assessment of the ML vulnerability related to mortgage credit shows that:

(a) risk exposure:
Mortgage credit is not exposed to an inherent high exposure to ML risks because, even if it involves high amounts, the financial transaction is executed through secured channels (credit institutions). It may be exposed to high risk customers (e.g. PEPs), and could involve cross-border transfers of funds.

(b) risk awareness:
Credit institutions are well aware about the ML risks - awareness which takes into account the fact that AML controls are exercised by different obliged entities who are engaged at different stages of the real estate purchase-loan approval process (credit institutions, mortgage brokers, real estate agents, notaries, lawyers). This is less the case when mortgage credit involves the real estate sector. The risk awareness is quite good due to the fact that the sector has put in place guidance to detect the relevant red flags on ML. This is confirmed by a good level of reporting. FIUs and LEAs are also well aware about the vulnerabilities of the sector.

(c) legal framework and controls:
Mortgage credit is included in the AML/CFT framework at EU level. Controls in place are considered as rather efficient when the mortgage credit is provided by credit institutions. However, when a real estate agent is concerned, the controls in place are less efficient. New risks and opportunities may emerge with FinTech/RegTech.

Conclusions: when provided by banks, mortgage credit products are as vulnerable as retail banking. However, most of the time, the interaction with the real estate sector makes the vulnerabilities higher. In that context, the level of ML vulnerability related to mortgage credit is considered as moderately significant (level 2).

Mitigating measures

- The Commission proposed to reinforce the Directive (EU) 2015/849 by putting forward targeted amendments as presented in the Commission's proposal adopted in July 2016 (see COM(2016)450):

  (i) broadening the scope and reinforcing accessibility of beneficial ownership information for legal entities and legal arrangements. This will also include interconnection of beneficial ownership registers at EU level.

(ii) clarifying explicitly that electronic identification means as set out in Regulation (EU) No 910/2014 ("e-IDAS") can be used for meeting CDD requirements

- The Commission will launch further analysis in order to identify risks and opportunities on FinTech/RegTech. The Commission FinTech Task Force will assess technological developments, technology enabled services and business models, will determine whether existing rules and policies are fit for purpose and will identify options and proposals to harness opportunities or address possible risks.

- The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed
- Updated guidelines on internal governance further clarifying expectations with regard to the functions of the compliance officer in financial institutions should be provided by the ESAs. The Commission services will further analyse whether those guidelines allow the position of the AML/CFT – compliance officer to be sufficiently reinforced.
- Member States should ensure that competent authorities/self-regulatory bodies supervising real estate sector produce an annual report on supervisory measures put in place to ensure that the sector accurately applies its AML/CFT obligations, in particular related to the check of source of funds (mortgage credits). When receiving suspicious transaction reports, self-regulatory bodies shall report annually on the number of reports filed to the FIUs.

Life-Insurance

Product
Life Insurance
Sector
Insurance sector
General description of the sector and related product/activity concerned
Life insurance companies offer a range of investment products, which include life insurance benefit as a component. The products can be structured as unit linked, or index linked products or other products with or without guarantees from the insurance company. According to the ECB statistical database the total assets of Insurance Corporations in the Euro area as at September 2015 were reported EUR 7022 billion[14]. According to data published by Insurance Europe, in 2015, European life premiums amounted to EUR 73 billion[15]. In addition to the AML Directive, specific provisions are aimed at mitigating risks shown by life insurance used as an investment vehicle. Article 59 Directive 2009/138/EC (Solvency2) and Article 323 Commission Delegated Regulation (EU) 2015/35 require an assessment whether there are reasonable grounds to suspect that, in connection with the qualifying holding of the shareholder or members having a qualifying holding in the special purpose vehicle, money laundering or terrorist financing is being or has been committed or attempted, or that the qualifying holding could increase the risk thereof.
Description of the risk scenario
Perpetrators are using fraud to life insurance products to fund their activities. Early redemption life policies to receive lump sums, particularly where product can be transferred Money laundering and terrorist financing risks in the insurance industry may be found in life insurance and annuity products. Such products allow a customer to place funds into the financial system and potentially disguise their criminal origin or to finance illegal activities. Relevant risk scenarios are typically focussed on investment products in life insurance (and not on death benefit products as such). The risks may arise or materialise through one or more of the following: 1. An insurer* accepts premium payment in cash. 2. An insurer refunds premiums upon policy cancellation or policy surrender to an account other than the source of original funding. 3. An insurer does not perform KYC due diligence in general and the source of investments in particular.

[14] https://www.insuranceeurope.eu/sites/default/files/attachments/European%20Insurance%20-%20Key%20Facts%20-%20August%202016.pdf

[15] http://www.insuranceeurope.eu/sites/default/files/attachments/European%20Insurance%20-%20Key%20Facts%20-%20August%202015.pdf

4. An insurer sells transferable policies (which are uncommon).

5. Investment transactions involve trusts, mandate holders, etc.

6. An insurer sells tailor made products, where the investor dictates the underlying investment or portfolio composition.

7. An insurer may sell a small investment policy initially; where the investor has the opportunity to make further large investment without additional KYC due diligence.

The risk of terrorist financing exists in 2, 4 and 6 above for direct and indirect financing of terrorist operations.

The risk of money laundering exists in all of the above. Perpetrators would use risk scenarios (1, 6 and 7) for placement, (2 and 4) for layering and (2, 4, 6 and 7) for integration.

*In all of the above examples, the process may involve the insurers or its agent or an intermediary. For simplicity of presentation, we will use the term "insurer".

Threat

Terrorist financing

The assessment of the TF threat related to life insurance shows that terrorist groups have vague intentions to use this modus operandi. It requires specific knowledge of the product and its specificities. Life insurance contracts are not easily accessible and require a lot of documentation to support the request which is quite dissuasive and less attractive for terrorist groups. One case can be considered: when life insurance is subscribed by foreign terrorist fighters who ask for the redemption of the life insurance funds for the benefit of their family in case of suicide or war. However, legislations in place in Member State do not allow this type of clause, which make the risk less important.

Conclusions: LEAs have limited evidence on life insurance misused for TF purposes. It requires knowledge and planning expertise which make this modus operandi rather unattractive. In that context, the level of TF threat related to life insurance is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to life insurance shows that organised crime organisations can use this modus operandi but it requires complex architecture to hide proceeds of crime (bank account wrapped in an insurance policy; multiple accounts in tax haven and loaded in cash, and used as guarantee to ask for a credit loan and then money sent to life insurance policy). Cases exist but they are few, and they require sophisticated planning and knowledge to make the life insurance a viable option.

Conclusions: some case of life insurance abused for ML purposes have been identified but most of the time, they are the result of sophisticated schemes. In that context, the level of ML threat related to life insurance is considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to life insurance shows that
(a) risk exposure:

When misused, life insurance is mostly used to place funds anonymously than to withdraw them. However, the risk exposure seems rather limited given the amount of transactions concerned.

(b) risk awareness:
The sector seems quite unaware about TF risks. STRs are most of the time sent quite late in the process, because life insurers tend to wait for the withdrawal of the funds to consider whether or not there is a suspicion.

(c) legal framework and controls:
Life insurance is included in the AML/CFT framework at EU level. New risks and opportunities may emerge with FinTech/RegTech.

Conclusions: risk awareness from the sector is low while the risk exposure is quite high. However, cases at stake are very limited and due to the limited attractiveness of the product, the level of TF vulnerability related to life insurance is considered as lowly significant/moderately significant (level 1- 2).

Money laundering

The assessment of the ML vulnerability related to life insurance shows that :
(a) risk exposure:
When misused, life insurance is mostly used to place funds anonymously than to withdraw them. However, the risk exposure seems rather limited given the amount of transactions concerned.

(b) risk awareness:
The sector is well aware about the ML risks.

(c) legal framework and controls:
Services are most of the time provided through bank accounts. Accurate controls generally apply for this type of products.

Conclusions: life insurance is currently well framed and the sector seems quite aware about the risk of ML abuses. The controls in place are correctly implemented. In that context, the level of ML vulnerability related to life insurance is considered as lowly/moderately significant (level 1-2). When life-insurance products are used as investment product for wealth management or other investment services, the respective risk level should be considered.

Mitigating measures

No further proposal is made at this stage

Non-Life Insurance

Product
Non-Life Insurance
Sector
Insurance sector
General description of the sector and related product/activity concerned
According to the EBA statistical database the total assets of Insurance Corporations in the Euro area as at September 2015 were reported EUR 7022 billion*. *Further breakdown by sub-activity is not available, but not essential from the perspective of AML/ATF. According to data published by Insurance Europe, in 2015, the largest non-life insurance market, motor insurance, totalled EUR132 billion in premiums, followed by health insurance with EUR119.3bn and property insurance market with EUR93 billion, accident insurance EUR32 billion and general liability insurance with EUR33.8 billion.%
Description of the risk scenario
Perpetrators are using fraud to insurance products to fund their activities (work place insurance, car insurance…) ML in non-life insurance can occur within the context of, and as the motive behind, insurance fraud, for example where this results in a claim to be made to recover part of the invested illegitimate funds. Relevant risk scenarios are typically focussed on high frequency premiums and cancellations. The risks may arise or materialise through one or more of the following: 1. An insurer* accepts premium payment in cash. 2. An insurer refunds premiums upon policy cancellation or policy surrender to an account other than the source of original funding. The risk of money laundering exists in all of the above. ML intent is to use the scenario 1 for placement and scenario 2 for layering/integration. *In all of the above examples, the process may involve the insurer or its agent or an intermediary. For simplicity of presentation, we will use the term "insurer". Similarly the risk of terrorist financing relates to insurance fraud to get access to sources of revenues for terrorist activities. Such schemes materialised in work place insurance and car insurance for instance.
Threat

Terrorist financing

The assessment of the TF threat related to non-life insurance (e.g. cars or workplaces) presents similarities with the assessment of the TF related to life-insurance. It is difficult to say that this modus operandi does not have any relevance but it requires, nevertheless, some planning and large paper trails which makes it not really attractive for terrorist groups, although some evidence has been gathered during the terrorist attacks. However, for sake of comparability, it presents the same level of TF threat.

Conclusions: LEAs have limited evidence on non-life insurance misused for TF purposes. It requires knowledge and planning expertise which make this modus operandi rather unattractive. In that context, the level of TF threat related to non-life insurance is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to non-life insurance (e.g. cars or workplaces) shows that, unlike TF, ML abuses of non –life insurance require sophisticated schemes which make the risk scenario not secure or attractive enough. LEAs have no specific evidence that non-life insurance has been used to launder proceeds of crime.

Conclusions: non-life insurance is not used for ML purposes as it requires planning and expertise which make this modus operandi rather unattractive. In that context, the level of ML threat related to non-life insurance is considered as lowly significant / non relevant (level 1).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to non-life insurance (e.g. cars or workplaces) shows that two cases may occur: (i) undeclared work in motor vehicles retails/ fraud on car insurances: funds coming from the fraud are sent by cash transfers; (ii) burning of cars to obtain insurance redemption.

(a) risk exposure:

The risk exposure is limited due to the fact that it necessarily concerns huge amounts of funds and that funds shall be accessed, with prior identification.

(b) risk awareness:

Generally speaking, non-life insurance is more vulnerable than life insurance because the sector is not necessarily aware about these risks (CDD are implemented and there is no record keeping) or does always trigger specific red flags on TF or ML. Insurance issuers tend to pay more attention at the moment of the pay-out, when the risk is perceived as bigger.

(c) legal framework and controls

Non-life insurance is not covered by the AML/CFT framework at EU level. Where Member States have put in place some regulations, controls seem to work adequately, including with systems of self-declarations.

Conclusions:. In many Member States, the legal frameworks in place have triggered some controls and have raised awareness within the sector. However, there are still some weaknesses in the detection of suspicious transactions and reporting. In that context, the level of TF vulnerability related to non-life insurance is considered as moderately significant (level 2).

Money laundering

The assessment of the ML vulnerability related to non-life insurance (e.g. cars or workplaces) shows that

(a) risk exposure:

Most of the time, non-life insurance is misused for ML purposes in a broader context of fraud (fake investment, empty shell).

(b) risk awareness:

The implementation of CDD is not widespread within the EU, but when Member States have an AML framework in place for non-life insurance, they notice that obliged entities tend to not apply any CDD at all. However, considering the number of cases concerned, there is no evidence that such weakness may increase the risk of ML

(c) legal framework and controls

There are no EU requirements to include non-life insurance in the scope of AML/FT. The non-life insurance framework depends on national legislations.

Conclusions: few cases on non-life insurance misuses for ML purposes have been identified. Most of the time, they are part of a broader fraud-scheme. In that context, the level of ML vulnerability related to non-life insurance is considered as lowly vulnerable (level 1)/ non relevant.

Mitigating measures

No further proposal is made at this stage

Safe custody services

Product
Safe custody services
Sector
Credit and financial sector and private security companies
Description of the risk scenario
Perpetrators rent multiple safe custody services (commercial or banking ones) to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a perpetrator establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system. Free zones may be used as shelter for illicit activities including proceeds from criminal activities.
Threat
Terrorist financing The assessment of the TF threat related to safe custody services has not been considered as relevant. In that context, the TF threat is not part of the assessment. **Conclusions: non relevant**
Money laundering The assessment of the ML threat related to safe custody services shows that this risk scenario presents the specificity that the value is stored and not necessarily converted. Then, it may not be financially attractive. However, it represents the possibility to hide proceeds of crime without any possibility to be detected. These "dormant" deposit's systems are, according to LEAs, increasingly used to safe deposits and to take assets out of the financial system. Exact data are nevertheless difficult to get because such safe custody services are also used for relatives. This constitutes an additional element to the ML threat considering that the person who has deposited funds is not necessarily the same who will withdraw them. The access by other persons to the funds increases the level of threat. It is also worth mentioning that market players other than banks are also providing such services (storage facilities) which extend the scope of tools available to criminal organisations. This also contributes to increase the level of threat. **Conclusions: many Member States have noticed an increasing trend in the use of the modus operandi by criminal organisations to hide proceeds of crime. Safe custody services are rather attractive because they do not require specific expertise and are a fairly secure tool to escape tax or AML controls. In that context, the level of ML threat related to safe deposits is considered as significant (level 3).**
Vulnerability
Terrorist financing The assessment of the TF vulnerability related to safe custody services has not been considered as particularly relevant. In that context, the TF vulnerability is not part of the assessment.

Conclusions: non relevant

Money laundering

The assessment of the ML vulnerability related to safe deposits shows that a distinction shall be done between services provided by credit institutions and those provided by non-banks entities (storage facilities).

(a) risk exposure:
In both cases, the risk exposure is high because large sums of cash may be at stake. This level of risk exposure may be increased by the nature of customers involved (high risk customers).

(b) risk awareness:
Concerning safe custody services provided by credit institutions, basic CDDs apply. Competent authorities are sometimes engaged in a proactive approach with the sector. Banks remain nevertheless vulnerable with regard to the "content" of the safe deposits boxes. Most of the time, they have no information on the funds placed in the safe deposits. In the case of private companies delivering such services, they do not all comply with AML/CFT requirements and some of them allow the rental of safe deposits with cash. Another question is whether the risk of ML occurs at the time of the storage already or only once the funds are inserted in the real economy. From a law enforcement perspective, the more the funds are stored, the easier the anonymity of the transaction is.

(c) legal framework and controls
Safe custody services or free zones shelters are not included, as such, in the AML/CFT legal framework at EU level. However, safe custody services provided by credit and financial institutions are included in the framework applicable to those obliged entities. Undertakings carrying out safe custody services as listed in point (14) of Annex I of Directive 2013/36/EU are specifically subject to AML/CFT rules. However financial institutions may not be in a position to carry out in practice their monitoring obligations and assessing the source of funds since they are not aware of the content of safe deposit boxes. In addition, this does not cover commercial storage companies or other storage facilities that may be used for similar services. In some countries, certain storage/safe services in general are regulated and supervised as such.

Conclusions: when provided by credit and financial institutions, safe custody services are subject to CDD requirements and controls. However, it is not always possible to understand exactly the source of funds and ongoing monitoring may have a blind spot since the content is usually unknown to the financial institution. In addition, these safe deposits may be accessible to third parties other than the initial customer which increases the vulnerability. The market is fragmented with the emergence of private entities and other commercial storage/safe services. In that context, the level of ML vulnerability is considered as moderately significant/significant (level 2-3).

Mitigating measures

- Member States should provide that credit and financial institutions offer safe custody services only for holders of a bank account in the same obliged entity – and address appropriately risks posed by access by third parties to safe deposit boxes. Member States should define measures commensurate to the risk posed by non-financial safe deposit providers, including in freeports, depending on the national circumstances.

Non-financial products

Creation legal entities and legal arrangements

Product/Service
Creation legal entities and legal arrangements
Sector
Trust or company service providers (TCSPs), Legal professionals, Tax advisors/accountants/auditors, Providers of service related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking = "professional intermediaries"
General description of the sector and related product/activity concerned
TCSPs, legal professionals, tax advisors/accountants and providers of services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking provide a wide range of services to individuals and businesses for commercial undertakings and wealth management. According to the Directive 2005/60/EC, obliged entities shall identify the beneficial owner when entering into a business relationship and taking risk-based and adequate measures to verify the identity of the beneficial owners as defined in Article 3(6). In addition to AML legislation, the following EU company law directives lay down general rules on setting up limited liability companies, especially with regard to capital and disclosure requirements. • **Directive 2009/101/EC** covers the **disclosure** of company documents, the validity of obligations entered into by a company, and nullity. It applies to all public and private limited liability companies. It replaces Directive 68/151/EEC (the 1st Company Law Directive). The current consolidated version includes amendments introduced by Directive 2003/58/EC (now repealed) and Directive 2012/17/EU. • **Directive 2012/30/EU** **covers** the **formation** of public limited liability companies and rules on **maintaining and altering their capital**. It sets the minimum capital requirement for EU public limited liability companies at EUR 25 000. It replaces Directive 77/91/EEC (the 2nd Company Law Directive). The consolidated version includes amendments introduced by Directive 2006/68/EC and Directive 2009/109/EC. • **Directive 89/666/EEC** (the 11th Company Law Directive) introduces disclosure requirements for **foreign branches** of companies. It covers EU companies which set up branches in another EU country or companies from non-EU countries setting up branches in the EU. • **Directive 2009/102/EC** (the 12th Company Law Directive) provides a framework for setting up a **single-member company** (in which all shares are held by a single shareholder). It covers private limited liability companies, but EU countries may decide to extend it to public limited liability companies. It replaces Directive 89/667/EEC. The rules on formation, capital and disclosure requirements are complemented by **accounting and financial reporting rules.** Listed companies must also meet certain **transparency requirements.**

Description of the risk scenario

Perpetrators create complex structures involving many jurisdictions, in particular offshore jurisdictions with secretive chains of ownership where the owner of another company or another legal structure is registered elsewhere. Nominees are designated and will only appear to be in charge of the company by hiding the link with the true beneficial owner. By involving offshore companies, the perpetrators can stay anonymous, return the funds derived from criminal activity into the legal economy, and commit tax fraud, tax evasion and other activities that impair the state budget or conceal the sources of the funds.

This involves the creation of 'opaque structures', defined as structures where the true identity of the owners(s) of entities and arrangements in that structure is concealed through the use of nominee directors for instance. In such cases, it is the nominee director who only appears to be the beneficial owners of the company[16]. These schemes make use of offshore jurisdictions which attract significant investments increasing by 7% in 2014 to reach 11 trillion USD[17].

General comment (where relevant)

For this risk scenario, the assessment covers legal entities such as companies, corporate structures, foundations, associations, non-for-profit organisations, charities and similar structures. It also covers legal arrangements such as trusts or other legal arrangements having a structure or functions similar to trusts (e.g. *fiducie*, *treuhand*, *fideicomiso* …). The risk assessment relates to the nature of the activity and not the structure as such. This approach does not deny the specific nature of legal entities versus legal arrangements (the latter does not have legal personality and remains basically a contractual relationship). However, as far as the nature of the service concerned (here the creation of the structure), these specificities do not make any key difference: legal entities and legal arrangements can be used the same way for hiding the true beneficial owners. Perpetrators favour a type of structure depending on the legal environment of a given jurisdictions, the perpetrators' type of expertise and convenience purposes. The creation is easily accessible by organised crime organisations for all these structures. In all cases, these structures could be vehicles used to create opaque and complex schemes which make it more difficult to identify the real owner and the real origin of the funds.

Threat

Terrorist financing

Perpetrators have an intent for setting up opaque structure which is needed for instance to circumvent restrictive measures in place. The assessment of the TF threat related to the creation of legal entities and legal arrangements shows that terrorist organisations may have some difficulties creating such kind of structures as these terrorist organisations are most of the time on sanctions list. The more the terrorist organisation wants to hide its beneficial ownership identity, the more sophisticated the process needs to be. Knowledge of both domestic and international regulatory and taxation rules are required to create these structures which entail a high level of knowledge that can be provided only by professional intermediaries. Nevertheless, some simplest cases have been identified by LEAs and FIUs,

[16] https://www.offshorebvi.com/offshore-company-management.php
https://www.theguardian.com/uk/2012/nov/25/offshore-trick-bvi-nominee-director

[17] https://www.bcgperspectives.com/content/articles/financial-institutions-growth-global-wealth-2015-winning-the-growth-game/?chapter=2%20-%20chapter2

through the use of bank accounts and professional intermediaries which allow the easy and fast creation of structures that may help gathering cash to finance terrorist activities. Thus, from the point of view of the capability, the creation of legal entities and legal arrangements can be considered as relevant for TF threat although a limited number of TF cases have been reported by law enforcement

Conclusions: while few cases of exploitation of this modus operandi for TF purposes have been identified, the technical expertise and knowledge required is high, and may thus dissuade terrorist organisations which may prefer simpler and more accessible solutions. In this context, the level of TF threat related to the creation of legal structures is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to the creation of legal entities and legal arrangements shows this tool is mainly and even quite exclusively used to hide and obscure the beneficial ownership. From the point of view of the costs, setting up a legal entity or a legal arrangement is rather straightforward and may be undertaken online. Some costs or higher level of expertise/planning may be required if the criminal organisations rely on intermediaries to create more complex structures, for instance involving more than one jurisdictions in order to better hide the true identities of the owners. Knowledge of domestic and international regulatory and taxation rules are required to create these structures which entail a high level knowledge that can be provided only by professional intermediaries. However, as far as the creation of the structure itself is concerned and as long as the use of intermediaries may suffice to hide the beneficial ownership, the use of this modus operandi is considered as an attractive and fairly secure way to launder proceed of crime. In addition, FIUs and LEAs consider that this modus operandi is recurrently used by criminal organisations.

Conclusions: although the creation of legal entities or legal arrangements cannot be isolated from the business activity itself, this risk scenario is considered as a lucrative tool to lauder proceeds of crime. In that context, the level of ML threat related to the creation of legal structures is considered as significant/very significant (level 3/4).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to the creation of legal entities or legal arrangements shows the following characteristics:

(a) risk exposure:
The main aspect of the risk exposure relates to the fact that legal entities and legal arrangements may, in certain circumstances, easily be created remotely and with no specific identification requirement (through unsecured delivery channels). In that context, the process may be fully anonymous and professional intermediaries may unwittingly be misused by terrorist groups located in high risk areas to create a structure with no legitimate purpose. In other situations, the non-face-face creation of the structures may involve professional intermediaries who are located outside the EU. In that case, the entry point to identify who the beneficial owner is remains the financial institution in charge of opening the bank account. Finally, some intermediaries or third parties may provide dedicated services to hide the beneficial ownership, impacting the whole profession which may be considered as complicit in the setting up of these TF schemes.

(b) risk awareness

In general, professional intermediaries seem to be aware about the risk of being misused by illegitimate requests to create legal entities and legal arrangements. The risk that these structures could be used to hide the beneficial owner is well known. However, given that in the TF context the creation of legal entities and legal arrangements may still rely on legitimate money, red flags are not triggered appropriately. Several professional sectors may be involved in the creation of these structures and competent authorities are not always able to deliver proper guidance to these professional sectors.

(c) legal framework and controls

Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking (since 2005) are subject to the EU anti-money laundering requirements.

Based on the level of STRs, competent authorities consider that controls in place are really low and elements gathered at the beginning of the business relationships are not developed enough to detect and analyse the TF risks related to the creation of legal entities or legal arrangements.

EU Members have different regulatory and taxation regimes that may be exploited by terrorist organisations. Enforcement of the requirements related to the identification of the beneficial owner at the beginning of the business relationship remains still an important challenge for obliged entities concerned and constitutes at this stage a gap in many EU AML/CFT regimes.

Concerning services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking, there is no information concerning their supervision by competent authorities and whether or not they comply with AML/CFT requirements.

Conclusions: although this modus operandi is not necessarily the one most used for terrorist financing, the TF vulnerability related to creation of legal structures is considered as significant/very significant (level 3/4).

Money laundering

The assessment of the ML vulnerability related to the creation of legal entities and legal arrangements shows that:

(a) risk exposure:

The main aspect of the risk exposure relates to the fact that legal entities and legal arrangements may, in certain circumstances, easily be created remotely and with no specific identification requirement (through unsecured delivery channels). In that context, the process may be fully anonymous and professional intermediaries may unwittingly be misused by criminal organisations located in high risk areas to create a structure with no legitimate purpose. In other situations, the non-face-face creation of the structures may involve professional intermediaries who are located outside the EU. In that case, the entry point to identify who the beneficial owner is remains the financial institution in charge of opening the bank account. Finally, some intermediaries or third parties may provide dedicated services to hide the beneficial ownership, impacting the whole profession which may be considered as complicit in the setting up of these ML schemes.

(b) risk awareness:
Both TCSPs and legal professions/tax advisors seem to be aware about the risk of illegitimate requests to create legal entities and legal arrangements. The risk that these structures could be used to hide the beneficial owner is well known. However, there are still important shortcomings in terms of enforcement. This is the case when several obliged entities are involved in the creation of structures and where the application of CDD, including who the beneficial owner is, relies on the financial sector which is not always well equipped to face situations where the beneficial owner is voluntarily hidden. There are also important shortcomings in terms of understanding, by the obliged entities, of their AML obligations or even knowledge of these obligations. This is particularly true for the use of common law legal arrangements, like trusts, which are not familiar to civil law countries and are not known in their national law or used as investments/business vehicles. Guidance and applicability of CDD is often not available in these civil law jurisdictions on how AML requirements should be applied to such legal arrangements.
The risk awareness of services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking is impossible to assess as there is no information available concerning whether or not they apply the AML/CFT requirements

(c) legal framework and controls
Legal framework: Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking (since 2005) are subject to the EU anti-money laundering requirements.
The current EU legal framework (3rd AMLD) requires the identification of the beneficial owner before entering into a business relationship but does not impose any requirement on the legal entity or the legal arrangement itself to disclose spontaneously its beneficial owner at the time of the creation – although other disclosure requirements exist for EU companies according to company law legislation.
EU Members have different regulatory and taxation regimes that are exploited by criminal organisations. These organisations may take advantage of more lenient AML/CFT frameworks concerning the identification of beneficial owners of legal entities and arrangements or of national regimes that do not provide for personal or corporate income tax.

Controls: In the absence of any EU requirement to disclose who the beneficial owner is at the time of the creation of the structure, in particular for complex structures covering many jurisdictions, controls are either not effective or do not exist, which means that opaque structures can be easily created to hide illegitimate funds. In addition, in several situations, competent authorities and FIUs have noticed the involvement of off-shore jurisdictions where the ability of LEAs to conduct investigations depends on the existence of MLA agreements with these jurisdictions. The consequence is that as long as there is no MLA agreement, the process to identify the beneficial ownership is hampered.
IT tools have been put in place to allow the creation of corporate structures in a speedy and anonymous way. In the case of legal arrangements, some of them can be contracted in a very informal way which creates additional obstacles for the controls.

As far as services offering advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of

undertaking, there is no information concerning their supervision by competent authorities and whether or not they comply with AML/CFT requirements.

<u>Conclusions</u>: the ML risk exposure surrounding the creation of legal entities or legal arrangements is considered as significant due to the level of anonymity and the characteristics of the customers and areas involved. The risk awareness of professional intermediaries seems theoretically rather satisfactory but it is not confirmed by the number of STRs which remains very low. There is a lack of robust AML/CFT framework in many Member States and relevant rules do not seem correctly understood. The legal framework is not adapted to the risk (beneficial ownership identification ex-post and not prior to the creation of the structure) and the controls are inexistent. In that context, the ML vulnerability related to the creation of legal entities, legal arrangements and non-profit organisations/charities is considered as <u>significant/very significant</u> (level 3/4).

Mitigating measures

<u>1) for competent authorities/self-regulatory bodies</u>

- Member States should ensure that competent authorities/self-regulatory bodies provide training sessions and guidance on risk factors with specific focus on non-face-to-face business relationships; off-shore professional intermediaries or customers or jurisdictions; complex/shell structures

- Member States should ensure that self-regulatory bodies/competent authorities conduct thematic inspections on how beneficial owner identification requirements are implemented

- Annual reports on the measures carried out to verify compliance by these obliged entities with their obligations related to customer due diligence, including beneficial ownership requirements, suspicious transaction reports and internal controls should be provided by competent authorities/self-regulatory bodies to Member States

- Member States should put in place some mechanisms to ensure that the creation of structures should be carried out under control of a professional (obliged entity), who should have to develop their due diligence.

- Member States should put in place some mechanisms allowing competent authorities and FIUs to identify the situations where:

(i) for legal entities: obliged entities have identified the senior manager as the beneficial owner, instead of the natural person who ultimately owns or controls the legal entity through direct or indirect ownership. In such case, obliged entities should keep record of any doubt that the person identified is the beneficial owner.
(ii) for legal arrangements: obliged entities should identify cases where the settlor, trustee, protector, beneficiaries or any other natural person exercising ultimate control over the trust involve one or several legal entities. In such cases, the obliged entities should also identify the beneficial owner of these legal entities.

- Member States should put in place mechanisms to ensure the information held in central beneficial ownership register is verified on a regular basis. For this purpose, a national authority should be designated to collect and check the information on the

beneficial owner. This national authority should receive from obliged entities any discrepancy that would be found between the beneficial ownership information held in the registers and the beneficial ownership information collected as part of their customer due diligence procedures. Where such discrepancies are not sufficiently justified by the legal structure or the legal arrangement, the national authority should provide for adequate pecuniary and/or administrative sanctions.

- Member States should ensure that providers of services offering advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking are properly regulated and supervised at national level and comply with their obligations on beneficial ownership.

2) from the Commission:
In the context of Commission's proposal COM(2016)450: reinforcing the transparency requirements for beneficial ownership information on legal entities and legal arrangements

Business activity of legal entities and legal arrangements

Product/Service
Business activity entities and legal arrangements
Sector
Trust or company service providers (TCSPs), Legal professionals, Tax advisors/accountants/auditors, Providers of service related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking = "professional intermediaries"
General description of the sector and related product/activity concerned
TCSPs, legal professionals, tax advisors/accountants and providers of services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking provide a wide range of services to individuals and businesses for commercial undertakings and wealth management. According to the Directive 2005/60/EC, obliged entities shall identify the beneficial owner when entering into a business relationship and taking risk-based and adequate measures to verify the identity of the beneficial owners as defined in Article 3(6). In addition to AML legislation, the following EU company law directives lay down general rules on setting up limited liability companies, especially with regard to capital and disclosure requirements. • **Directive 2009/101/EC** covers the **disclosure** of company documents, the validity of obligations entered into by a company, and nullity. It applies to all public and private limited liability companies. It replaces Directive 68/151/EEC (the 1st Company Law Directive). The current consolidated version includes amendments introduced by Directive 2003/58/EC (now repealed) and Directive 2012/17/EU. • **Directive 2012/30/EU** **covers** the **formation** of public limited liability companies and rules on **maintaining and altering their capital**. It sets the minimum capital requirement for EU public limited liability companies at EUR 25 000.It replaces Directive 77/91/EEC (the 2nd Company Law Directive). The consolidated version includes amendments introduced by Directive 2006/68/EC and Directive 2009/109/EC. • **Directive 89/666/EEC** (the 11th Company Law Directive) introduces disclosure requirements for **foreign branches** of companies. It covers EU companies which set up branches in another EU country or companies from non-EU countries setting up branches in the EU. • **Directive 2009/102/EC** (the 12th Company Law Directive) provides a framework for setting up a **single-member company** (in which all shares are held by a single shareholder). It covers private limited liability companies, but EU countries may decide to extend it to public limited liability companies. It replaces Directive 89/667/EEC. The rules on formation, capital and disclosure requirements are complemented by **accounting and financial reporting rules.** Listed companies must also meet certain **transparency requirements.**

Description of the risk scenario

Front companies used for fraud via false invoicing: Perpetrators use front company to apply false invoices to imported items, with the overpayments siphoned off to terrorist causes.

Trade based money laundering: Perpetrators use Trade based money laundering (TBML) as a means of justifying the movement of criminal proceeds through banking channels (via letter of credit, invoices) or through the use of global transactions, often using false documents regarding the trade of goods and services. It can potentially allow the rapid transfer of large sums by justifying an alleged economic purpose. TBML schemes have also been used by international terrorist groups with complex funding methods[18].

False loans: companies set up fictitious loans between them in order to create an information trail to justify transfers of funds of illegal origin. Perpetrators use fictitious loans as a mean for justifying movement of criminal proceeds through banking channels - without any economic reality.

In terms of legislation in place, the EU has adopted several accounting Directives as well as audit requirements to ensure that companies' accounts represent a true and fair view.

General comment (where appropriate)

For this risk scenario, the assessment covers legal entities such as companies, corporate structures, foundations, associations, non-for-profit organisations, charities and similar structures. It also covers legal arrangements such as trusts or other legal arrangements having a structure or functions similar to trusts (e.g. *fiducie*, *treuhand*, *fideicomiso* …). The risk assessment relates to the nature of the activity and not the structure as such. This approach does not deny the specific nature of legal entities versus legal arrangements (the latter does not have legal personality and remains basically a contractual relationship). However, as far as the nature of the service concerned (here the creation of the structure), these specificities do not make any key difference: legal entities and legal arrangements can be used the same way for hiding the true beneficial owners. Perpetrators favour a type of structure depending on the legal environment of a given jurisdictions, the perpetrators' type of expertise and convenience purposes. The creation is easily accessible by organised crime organisations for all these structures. In all cases, these structures could be vehicles used to create opaque and complex schemes which make it more difficult to identify the real owner and the real origin of the funds.

Threat

Terrorist financing

The assessment of the TF threat related to business activities of legal entities or legal arrangements shows that terrorists groups do not particularly favour this kind of modus operandi to finance terrorist activities. According to law enforcement authorities, this risk scenario is not really attractive for terrorists groups as it requires firstly the creation of an opaque structure (illicit legal entity or legal arrangement) or the infiltration of the ownership of a legitimate legal entity or legal arrangement. It requires planning and expertise capabilities. Due to the different steps to be accomplished, it is unlikely that "clean" money can be collected from this modus operandi in a speedy manner. However if perpetrators

[18] DEA and European Authorities Uncover Massive Hezbollah Drug and Money Laundering Scheme,", DEA - 1 February 2016: a case of the Lebanese group Hezbollah laundering significant proceeds from drug trafficking in Europe as part of a trade based money laundering scheme known as the Black Market Peso Exchange.

possess the expertise, they can use this modus operandi for money remittance instead of other classical techniques (money value transfer services, hawala etc). The modus operandi can become attractive if there is a need to transfer large volume of funds for TF purposes. Hence, terrorist groups may have some intentions to use it.

Conclusions: on the basis of the elements gathered from law enforcement authorities and financial intelligence units, the level of TF threat related to business activities business activities of legal entities and legal arrangements is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to business activities of legal entities or legal arrangements shows that the most widespread means to launder proceeds of crime used by organised crime organisations is trade-based money laundering and false invoicing. These illicit operations allow legitimate funds to be taken out of the company's cash flow: (i) by using forged invoices; (ii) by reducing the base for tax calculation; (iii) by reducing income tax by taking legitimate funds from the company; (iv) by laundering illegitimate proceeds by withdrawing cash from another company's account using intermediaries. While the level of expertise or planning capacities is not negligible, law enforcement authorities and financial intelligence units consider that organised crime organisations have recurrently exploited this modus operandi because it is generally quite easily accessible, has a low cost and is relatively easy to abuse. However, this modus operandi also involves several sectors at the same time: transfers of money through companies' structures generally are processed through the banking sector, and in many cases lawyers are identified as facilitators

Conclusions: while this modus operandi may require moderate levels of technical expertise and knowledge to build a TBML scheme, numerous cases have been identified by FIUs and LEAs which tend to demonstrate that it is quite easy to access and to abuse. On this basis, the level of ML threat related to business activities business activities of legal entities and legal arrangements and based on TBML is considered as very significant (level 4)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to business activities of legal entities or legal arrangements shows that:

(a) risk exposure
Significant sums can be gathered through business activities to finance terrorist organisations and activities. This business activity is most of the time cash based and could involve cross-border transactions with high-risk third countries.

(b) risk awareness:
Both TCSPs and legal professions/tax advisors seem to be aware about the risk to be misused to create legal entities and legal arrangements for illegitimate purposes linked to ML/TF. The risk that these structures could be used to hide the beneficial owner is well known. However, there are still important shortcomings in terms of understanding of their AML/CFT obligations, or even knowledge of them. In particular, given that in the context of TF, business activity can still rely on legitimate money, this does not necessarily trigger any red flags. Controls in place are then quite low and the consequence is that FIUs can detect and analyse the TF risks related to business activity through legal entities or legal

arrangements only in limited circumstances. Many professional sectors may be involved in the creation of legal structures and competent authorities are not always able to deliver proper guidance to these professional sectors.

(c) legal framework and controls

Legal framework: Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking (since 2005) are subject to the EU anti-money laundering requirements. These EU requirements impose that the beneficial owner of a legal structure or a legal arrangement, including non-profit organisations or foundations is identified before starting the business relationship. Despite this legal obligation, national regimes still present important gaps. In addition, accountant and auditors are applying accounting rules to ensure that company accounts represent a true and fair view.

Controls:

Based on the level of STRs, competent authorities consider that controls in place are very low and elements gathered at the beginning of the business relationships are not sufficiently developed to detect and analyse the TF risks related to the creation the and activities of legal entities and legal arrangements.

As far as services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking, there is no information concerning their supervision by competent authorities and whether or not they comply with AML/CFT requirements.

Conclusions: on the basis of the elements gathered and while this modus operandi is not necessarily the most obvious vehicle for terrorist financing, the TF vulnerability related to business activities of legal entities and legal arrangements is considered as significant (level 3).

Money laundering

The assessment of the ML vulnerability related to business activities of legal entities and legal arrangements shows

(a) risk exposure:

False loans are not a negligible phenomenon which is used widely by organised crime organisations. In certain cases, TMBL may imply large international trade transactions less easy to detect by banks. This difficult detection can be increased by the recurring use of strawmen which may impact on the level of vulnerabilities.

(b) risk awareness

Both TCSPs and legal professions/tax advisors seem to be aware about the risk to be misused to create legal entities and legal arrangements for illegitimate purposes linked to ML/TF. The risk that these structures could be used to hide the beneficial owner is well known. TCSPs are, in general, aware that they are not supposed to deal with third parties without having the correct compliance in place. However, the transactions at stake are rather complex (cross-border in particular) which make harder the investigation work of LEAs. Illicit origin of the funds is generally difficult to prove due to the multiplicity of actors,

geographical areas and channels used. Suspicious transactions are then quite difficult to detect (TMBL and false invoicing).

(c) legal framework and controls

Legal framework: Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking (since 2005) are subject to the EU anti-money laundering requirements. These EU requirements impose that the beneficial owner of a legal structure or a legal arrangement, including non-profit organisations or foundations is identified before starting the business relationship. Despite this legal obligation, national regimes still present important gaps. In addition, accountant and auditors are applying accounting rules to ensure that the companies account represent a true and fair view.

Controls: in several situations, competent authorities and FIUs have noticed the involvement of off-shore jurisdictions where the ability of LEAs to conduct investigations depends on the existence of MLA agreements with these jurisdictions. The consequence is that as long as there is no MLA agreement, the process to identify the beneficial ownership is terminated.

Concerning services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking, there is no information concerning their supervision by competent authorities and whether or not they comply with AML/CFT requirements.

Conclusion: the risk exposure of the sector is considered as very significant due to the lack of a robust ML framework in many jurisdictions especially rules on the identification of beneficial owners, which means that controls are inexistent in opaque structures involving many jurisdictions. In addition there is no information on whether the sector complies with AML.CFT requirements. On this basis, the level of ML vulnerability related to business activities through a legal structure and based on TBML is considered as significant (level 3)

Mitigating measures

1) for competent authorities/self-regulatory bodies

- competent authorities/self-regulatory bodies should provide training sessions and guidance on risk factors with specific focus on non-face-to-face business relationships; off-shore professional intermediaries or customers or jurisdictions; complex/shell structures
- self-regulatory bodies/competent authorities should conduct thematic inspections on how beneficial owner identification requirements are implemented
- Annual reports on the measures carried out to verify compliance by these obliged entities with their obligations related to customer due diligence, including beneficial ownership requirements, suspicious transaction reports and internal controls.

Mechanisms to ensure that the purchase/merger of a legal structure is carried out under control of a professional (obliged entity), who should have to develop their due diligence

- Member States should put in place some mechanisms allowing competent authorities and FIUs to identify the situations where:

(i) for legal entities: obliged entities have identified the senior manager as the beneficial owner, instead of the natural person who ultimately owns or controls the legal entity through direct or indirect ownership. In such case, obliged entities should keep record of any doubt

that the person identified is the beneficial owner.
(ii) for legal arrangements: obliged entities should identify cases where the settlor, trustee, protector, beneficiaries or any other natural person exercising ultimate control over the trust involve one or several legal entities. In such cases, the obliged entities should also identify the beneficial owner of these legal entities.

- Member States should put in place mechanisms to ensure the information held in central beneficial ownership register is verified on a regular basis. For this purpose, a national authority should be designated to collect and check the information on the beneficial owner. This national authority should receive from obliged entities any discrepancy that would be found between the beneficial ownership information held in the registers and the beneficial ownership information collected as part of their customer due diligence procedures. Where such discrepancies are not sufficiently justified by the legal structure or the legal arrangement, the national authority should provide for adequate pecuniary and/or administrative sanctions.
- Member States should ensure that providers of service related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking are properly regulated and supervised at national level and comply with their obligations on beneficial ownership.

<u>2) from the Commission:</u>

- In the context of Commission's proposal COM(2016)450: reinforcing the transparency requirements for beneficial ownership information on legal entities and legal arrangements

Termination of legal entities and legal arrangements

Product
Termination business activity of legal entities and legal arrangements
Sector
Trust or company service providers (TCSPs), Legal professionals, Tax advisors/accountants/auditors, Providers of service related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking = "professional intermediaries"
General description of the sector and related product/activity concerned

TCSPs, legal professionals, tax advisors/accountants and providers of service related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking provide a wide range of services to individuals and businesses for commercial undertakings and wealth management.

According to the Directive 2005/60/EC, obliged entities shall identify the beneficial owner when entering into a business relationship and taking risk-based and adequate measures to verify the identity of the beneficial owners as defined in Article 3(6).

In addition to AML legislation, the following EU company law directives lay down general rules on setting up limited liability companies, especially with regard to capital and disclosure requirements.

- **Directive 2009/101/EC** covers the **disclosure** of company documents, the validity of obligations entered into by a company, and nullity. It applies to all public and private limited liability companies. It replaces Directive 68/151/EEC (the 1st Company Law Directive). The current consolidated version includes amendments introduced by Directive 2003/58/EC (now repealed) and Directive 2012/17/EU.
- **Directive 2012/30/EU** **covers** the **formation** of public limited liability companies and rules on **maintaining and altering their capital**. It sets the minimum capital requirement for EU public limited liability companies at EUR 25 000.It replaces Directive 77/91/EEC (the 2nd Company Law Directive). The consolidated version includes amendments introduced by Directive 2006/68/EC and Directive 2009/109/EC.
- **Directive 89/666/EEC** (the 11th Company Law Directive) introduces disclosure requirements for **foreign branches** of companies. It covers EU companies which set up branches in another EU country or companies from non-EU countries setting up branches in the EU.
- **Directive 2009/102/EC** (the 12th Company Law Directive) provides a framework for setting up a **single-member company** (in which all shares are held by a single shareholder). It covers private limited liability companies, but EU countries may decide to extend it to public limited liability companies. It replaces Directive 89/667/EEC.

The rules on formation, capital and disclosure requirements are complemented by **accounting and financial reporting rules**.

Listed companies must also meet certain **transparency requirements.**

Description of the risk scenario
Fraud using bankruptcy/judicial liquidation of a company: following the bankruptcy of a company, the same company is bought by a former shareholder who creates a new structure to pursue the same business activity without financial difficulties anymore. Perpetrators cash out funds from the front company before the illegal activities are detected or before assets are seized by competent authorities.
General comment
For this risk scenario, the assessment covers legal entities such as companies, corporate structures, foundations, associations, non-for-profit organisations, charities and similar structures. It also covers legal arrangements such as trusts or other legal arrangements having a structure or functions similar to trusts (e.g. *fiducie*, *treuhand*, *fideicomiso* …). The risk assessment relates to the nature of the activity and not the structure as such. This approach does not deny the specific nature of legal entities versus legal arrangements (the latter does not have legal personality and remains basically a contractual relationship). However, as far as the nature of the service concerned (here the creation of the structure), these specificities do not make any key difference: legal entities and legal arrangements can be used the same way for hiding the true beneficial owners. Perpetrators favour a type of structure depending on the legal environment of a given jurisdictions, the perpetrators' type of expertise and convenience purposes. The creation is easily accessible by organised crime organisations for all these structures. In all cases, these structures could be vehicles used to create opaque and complex schemes which make it more difficult to identify the real owner and the real origin of the funds.
Threat
Terrorist financing The assessment of the TF threat related to termination of business activity has been considered in conjunction with ML schemes related to termination of business activity in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment. **Conclusion: in that context, the assessment of the TF threat related to termination of activities is considered as lowly/moderately significant (level 1/2).**
Money laundering The assessment of the ML threat related to the termination of business activity through legal structures shows that bankruptcy is part of a more global process and some judicial administrators have reported cases where false bankruptcy has been used to launder proceeds of crime. However, few cases have been identified by law enforcement authorities. This tends to demonstrate that criminal organisations perceive this modus operandi as unattractive or difficult to access as it requires some logistical and planning capabilities. **Conclusions: on the basis of the elements gathered during the assessment phase, the level of ML threat related to termination of business activity is considered as lowly/moderately significant (level 1/2).**
Vulnerability
Terrorist financing The assessment of the TF vulnerabilities related to termination of business activity has been considered in conjunction with ML schemes related to termination of business activity in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from

a separate assessment.

Conclusions: in that context, the level of vulnerability is moderately significant (level 2)

Money laundering

The assessment of the ML vulnerability related to the termination of business activity through legal structures shows that:

(a) risk exposure
Situations where termination of a business activity is at stake generally starts from a fraud.

(b) risk awareness
The detection of this modus operandi by LEAs and FIUs is easy given that most of the time it starts from a fraud. This predicate offence triggers the red flags for either the sector or the competent authorities. In general, bankruptcy is complex to elaborate and obliged entities (banks in particular) pay particular attention to such scenarios which are most of the time considered as suspicious.

(c) legal framework and controls
Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking (since 2005) are subject to the EU anti-money laundering requirements.
There is no specific provision related to this situation in the EU AML framework, but the number of STRs received tends to show that controls in place are efficient and allow the detection of the suspicion situations. Insolvency Directors managing an insolvency procedure also represent an additional control element.

As far as services related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking are concerned, there is no information concerning their supervision by competent authorities and whether or not they comply with AML.CFT requirements.

Conclusions: while bankruptcy is an issue for some Member States, the detection of such cases and the level awareness of the sector and other obliged entities allow considering that the level of vulnerability is moderately significant (level 2)

Mitigating measures

A/ if the termination is related to the creation of another legal entity or legal arrangements
1) for competent authorities/self-regulatory bodies

- Member States should ensure that competent authorities/self-regulatory bodies provide training sessions and guidance on risk factors with specific focus on non-face-to-face business relationships; off-shore professional intermediaries or customers or jurisdictions; complex/shell structures

- Member States should ensure that self-regulatory bodies/competent authorities conduct thematic inspections on how beneficial owner identification requirements are implemented

- Annual reports on the measures carried out to verify compliance by these obliged entities with their obligations related to customer due diligence, including beneficial ownership requirements, suspicious transaction reports and internal controls should be provided by competent authorities/self-regulatory bodies to Member States

- Member States should put in place some mechanisms to ensure that the creation of structures should be carried out under control of a professional (obliged entity), who should have to develop their due diligence.

- Member States should put in place some mechanisms allowing competent authorities and FIUs to identify the situations where:

(i) for legal entities: obliged entities have identified the senior manager as the beneficial owner, instead of the natural person who ultimately owns or controls the legal entity through direct or indirect ownership. In such case, obliged entities should keep record of any doubt that the person identified is the beneficial owner.
(ii) for legal arrangements: obliged entities should identify cases where the settlor, trustee, protector, beneficiaries or any other natural person exercising ultimate control over the trust involve one or several legal entities. In such cases, the obliged entities should also identify the beneficial owner of these legal entities.

- Member States should put in place mechanisms to ensure the information held in central beneficial ownership register is verified on a regular basis. For this purpose, a national authority should be designated to collect and check the information on the beneficial owner. This national authority should receive from obliged entities any discrepancy that would be found between the beneficial ownership information held in the registers and the beneficial ownership information collected as part of their customer due diligence procedures. Where such discrepancies are not sufficiently justified by the legal structure or the legal arrangement, the national authority should provide for adequate pecuniary and/or administrative sanctions.

- Member States should ensure that providers of services offering advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking are properly regulated and supervised at national level and comply with their obligations on beneficial ownership.

2) from the Commission:
In the context of Commission's proposal COM(2016)450: reinforcing the transparency requirements for beneficial ownership information on legal entities and legal arrangements

B/ if the termination is related to the purchase of another legal entity or legal arrangements

1) for competent authorities/self-regulatory bodies

- competent authorities/self-regulatory bodies should provide training sessions and guidance on risk factors with specific focus on non-face-to-face business relationships; off-shore professional intermediaries or customers or jurisdictions; complex/shell structures
- self-regulatory bodies/competent authorities should conduct thematic inspections on

how beneficial owner identification requirements are implemented

- Annual reports on the measures carried out to verify compliance by these obliged entities with their obligations related to customer due diligence, including beneficial ownership requirements, suspicious transaction reports and internal controls.

Mechanisms to ensure that the purchase/merger of a legal structure is carried out under control of a professional (obliged entity), who should have to develop their due diligence

- Member States should put in place some mechanisms allowing competent authorities and FIUs to identify the situations where:

(i) for legal entities: obliged entities have identified the senior manager as the beneficial owner, instead of the natural person who ultimately owns or controls the legal entity through direct or indirect ownership. In such case, obliged entities should keep record of any doubt that the person identified is the beneficial owner.

(ii) for legal arrangements: obliged entities should identify cases where the settlor, trustee, protector, beneficiaries or any other natural person exercising ultimate control over the trust involve one or several legal entities. In such cases, the obliged entities should also identify the beneficial owner of these legal entities.

- Member States should put in place mechanisms to ensure the information held in central beneficial ownership register is verified on a regular basis. For this purpose, a national authority should be designated to collect and check the information on the beneficial owner. This national authority should receive from obliged entities any discrepancy that would be found between the beneficial ownership information held in the registers and the beneficial ownership information collected as part of their customer due diligence procedures. Where such discrepancies are not sufficiently justified by the legal structure or the legal arrangement, the national authority should provide for adequate pecuniary and/or administrative sanctions.
- Member States should ensure that providers of service related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertaking are properly regulated and supervised at national level and comply with their obligations on beneficial ownership.

<u>2) from the Commission:</u>

- In the context of Commission's proposal COM(2016)450: reinforcing the transparency requirements for beneficial ownership information on legal entities and legal arrangements

High value goods – artefacts and antiquities

Product

High value goods - artefacts and antiquities

Sector

High value dealers

Description of the risk scenario

Terrorist financing - Perpetrators earn revenue from the sale of looted artefacts and antiquities. The trafficking in cultural goods is among the biggest criminal trades, estimated to be the third or fourth largest, and despite the fact that there are hardly any instruments for measuring this trade or any data on illicit commerce.

It is estimated that only 30-40% of antique dealings take place through auction houses where the pieces are published in catalogues; the rest occur through private transactions. On the whole, the total financial value of the antiquities market ranks third after drug and arms trafficking and amounts to up to $6 billion yearly.

Money laundering – Perpetrators convert proceeds of criminal activities into antiques and art goods to store or move these assets more easily.

Threat

Terrorist financing

The assessment of the TF threat related to the trafficking of looted artefacts and antiques shows that LEAs have identified cases of trafficking of looted antiquities within the EU. Several investigations have been conducted by Member States' LEAs where underlying trafficking in goods taken out of conflict zones (Iraq/Syria) via involvement of far east countries was used to hide more easily the provenance of goods. The portion of illegal market is, of course, to be considered but is by definition difficult to detect. From national studies conducted so far, it appears that the main threat comes from looting such products in third countries, notably in conflict zones such as Syria, and imposing taxes on these activities by terrorist organisations controlling the territory. For example, "rather than trading artefacts, Islamic State is earning money from selling digging permits and charging transit fees"[19]. Terrorists do not themselves "sell" the products to obtain revenues. Since the products might be sold in the EU by intermediaries, there is an indirect risk of financing terrorism.

From the intent and capability point of view, this risk scenario represents a financially viable option considering that looting of artefacts may produce a substantial amount of revenue. However, this modus operandi is not easy to use: it requires access to the illegal/dark economy; technical expertise and knowledge of the art market are also required and are not in the capability of every kind of terrorist group; the transportation of such products is not secure and not discrete enough. The conversion in cash of such products requires in any case planning capabilities which are not consistent with terrorist groups needs to access cash in a speedy way.

The international dimension of such threat cannot be excluded from the threat analysis. Law

[19] Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes, ICSR, 2017

enforcement authorities as well as UN have reported evidence that artefact looting and trafficking occur in conflicts zone. Such activities produce financial revenues that can be used by returning foreign terrorist fighters to commit terrorist acts in the EU territory.

Conclusion: at this stage, there is limited/no evidence that such scenario is used to finance terrorist activities in the EU. However, it represents an attractive source of revenue for organisations controlling territory in conflict zones, which could then be used to finance terrorist activities in the EU. Nevertheless, the level of knowledge, expertise and planning capabilities required reduces the level of threat. In that context, the level of TF threat related to the trafficking of artefacts and antiques is considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to the trafficking of looted artefacts and antiques shows that this risk scenario may present an interest for organised crime organisations when these "products" are converted into cash to launder proceeds of crime or evade tax. From LEAs point of view, this kind of traffic occurs mostly in Freeport zones making it more difficult to measure the extent of the phenomenon. There is little evidence that organised crime organisations use this modus operandi which in any case requires expertise and knowledge to sell these products at the best price. The illegal economy also plays a role in this risk scenario but is, by definition, difficult to assess.

Conclusions: this risk scenario may represent an attractive tool to convert proceeds of crime in clean cash. However, it requires high level of expertise and is not really secure for organised crime organisations. In that context, the level of ML threat related to the trafficking of artefacts and antiques is considered as moderately significant (level 2)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to the trafficking of looted artefacts and antiques shows that this risk is currently only an emerging one but vulnerabilities of the sector may increase in the short term. In the current context, the fruits derived from looting may be repatriated in the EU.

(a) risk exposure:

Investigations show that antiquities are offered to EU collectors from various third countries, generally through Internet auction sites or specialized online stores. Terrorist organisations may use concealment measures, such as IP-address spoofing, which makes it difficult to identify and determine the actual location of the seller. Exploitation of social media is also identified as more and more frequent tool so as to cut out the middleman and sell artefacts directly to buyers. Preference is given to cash transactions (sometimes for high amount) but online transactions are also widespread with no possibility for the financial institution to identify to real owner/buyer of the antiquities. Artefacts and antiques markets are sensitive, based on informal negotiations and trading where there is no specific monitoring of the transactions.

(b) risk awareness

According to LEAs, cultural artefacts do not land on EU territory or remain undetected. This

tends to demonstrate that competent authorities and FIUs visibility on such phenomenon is very low. Obliged entities do not undertake any record keeping (e.g. the origin of artefacts, to whom they are sold….) and there is not reporting. Customs authorities have difficulties detecting the illicit origin of cultural artefacts.

(c) legal framework and controls

AML framework: under the current AML EU framework, persons trading in goods are subject to EU AML requirements when they receive payments in cash in an amount of EUR15 000. This requirement focuses then on payments in cash without any consideration for risks posed by transactions using other means of payment. The EU AML does not target specifically artefacts and antiques neither from a product or merchant perspectives.

Ad hoc EU trade prohibitions: the EU has adopted ad hoc measures concerning importation of cultural goods into the custom territory from Syria and Iraq: Council Regulation (EC) No 1210/2003 of 7 July 2003 concerns certain specific restrictions on economic and financial relations with Iraq and Council Regulation (EU) No 36/2012 concerning restrictive measures in view of the situation in Syria prohibit trade in cultural goods with these countries where there are reasonable grounds to suspect that the goods have been removed without the consent of their legitimate owner or have been removed in breach of national or international law. However, competent authorities still have difficulties in tracking any good originating in these countries and the application of these Regulations may sometimes be challenging because of the nature of the products. It is nevertheless interesting to note that for those Member States who managed to seize cultural goods originating from Iraq or Syria, this is taken care of by the very same institutions controlling the general importation of cultural goods without generating any administrative burden of implementation, as the implementation of these rules form part of the daily work of the competent authorities.
In any case, while some EU rules exist, there are limited to specific regions and do not cover all cases of imports of cultural goods. This results in controls that are not sufficient to address the risks.

Conclusions: although there is little evidence that such risk scenario is used in the EU, it appears that the risk exposure is currently only emerging but may increase due to the geopolitical context. The legal framework does not allow an efficient monitoring of such transactions due to the fact that obliged entities are not aware of this TF vulnerability (no reporting, no record keeping). In that context, the level of TF vulnerability related to purchase of artefacts and antiques is considered as significant/very significant (level 3/4).

Money laundering

The assessment of the ML vulnerability related to the trafficking of looted artefacts and antiques shows that:

(a) risk exposure:

Given the sensitiveness of the artefacts and antiques market, it tends to favour informal channels where there is no specific security or monitoring of the transactions. It involves payments by cash (sometimes for high amounts) where the identification of the buyer is almost impossible.

(b) risk awareness

The sector seems more aware about the ML risk than the TF ones. In several Member States,

high value dealers receive relevant training and guidance. However, there is a very low level of STR reporting which raises questions with regard to the risk understanding.

(c) legal framework and controls

Persons trading in goods are subject to EU AML requirements when they receive payments in cash of EUR15 000 or more. In addition, in many Member States regulations aiming at limiting cash payments have been put in place. However, as it is the case for TF, controls in place are not sufficient to address the risks this product may present.

It is also important to mention that G7 members have considered that further work must be undertaken in that respect and that artefacts trafficking represent a high risk.

Conclusions: despite the fact that the risk awareness is higher than for TF, the other elements of the assessment present commonalities: low level of reporting, no evidence that cash payment limitations have limited the risks. In that context, the level of ML vulnerability related to purchase of artefacts and antiques is considered as significant/very significant (level 3/4).

Mitigating measures:

1) For the Commission:

- An impact assessment for a possible initiative to swiftly reinforce the EU framework on the prevention of terrorism financing by enhancing transparency of cash payments through an introduction of a restriction of cash payments or by any other appropriate means. By restricting the possibilities to use cash, the proposal would contribute to disrupt the financing of terrorism, as the need to use non anonymous means of payment would either deter the activity or contribute to its easier detection and investigation. Any such proposal would also aim at harmonising restrictions across the Union, thus creating a level playing field for businesses and removing distortions of competition in the internal market. It would additionally foster the fight against money laundering, tax fraud and organised crime.

- Member States should notify the measures applied by dealers in goods covered by the AMLD to comply with their AML/CFT obligations. On this basis, the Commission could further assess risks posed by providers of service accepting cash payments. It will further assess the added value and benefit for making additional sectors subject to AML/CFT rules.

2) For Member States:

- Member States should take due consideration of the risks posed by payment in cash in their national risk assessments in order to define appropriate mitigating measures such as the introduction of cash limits for payments, Cash Transaction Reporting systems, or any other measures suitable to address the risk. Member States should consider making sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of their NRA.

- Member States should ensure the provision of training actions for customs officers and the exchange of information and co-operation between customs and other authorities.

- Promoting authorisation requirements either in the country of export and/or in the EU, or self-declaration requirements, i.e. declaration by the EU importer that the good has exited the country of export in accordance with its laws and regulations.

- Awareness campaign and promotion of measures to the art market and museums, such as inventorying obligations and the formal recognition by the EU of existing codes of ethics or conduct for museum and the art market.

3) <u>For obliged entities</u>

- Promoting the use of written contracts to get a very detailed invoice with a clear description of the goods (value, product description...)

High value assets – Precious metals and precious stones

Product

High value assets- Gold and Diamonds

Sector

High value dealers

General description of the sector and related product/activity concerned

In the EU, the diamond market is mostly present in one country. The Belgian diamond dealers represent the most prevalent part of the diamond market in the EU. 1700 companies are officially registered with the Federal Public Service of Economy as diamond traders (total imports and exports in 2015 amounted 48 billion USD in Belgium). The world's largest mining companies have an office in Antwerp and sell a large share of their productions directly to Belgian companies. Belgium has 4 diamond bourses that are members of the World Federation of Diamond Bourses.

Specialised financial institutions provide liquidity to the diamond trade. Diamond-trading companies need this kind of financing to purchase large quantities of rough diamonds and to finance the manufacturing of these goods into polished diamonds.

Description of the risk scenario

Proceeds of crime (e.g. drug trafficking) are either moved to another country to purchase gold and jewellery which are sold in a third country on the basis of false invoices and certificates, or used directly to buy gold on the national territory and sold to a precious metals broker who then sold it to other businesses. Proceeds of the sale may then be wired to a third party to finance new criminal operations. Criminals favour precious metals and stones which are easy to store and to convert at small costs – which is typically gold and diamonds.

Threat

Terrorist financing

The assessment of the TF threat related to purchase of gold and diamonds shows that terrorists have exploited this modus operandi which is easily accessible and represents a financially viable option. It requires moderate level of planning and expertise. Gold is commonly used in war zones and is very attractive for terrorists groups.

Conclusions: the level of TF threat related to purchase of gold and diamonds is considered as moderately significant/ significant (level 2-3).

Money laundering

The assessment of the ML threat related to purchase of gold and diamonds shows that large ML schemes occurred through this scenario. From analysis already conducted (FATF), it appears that this scenario is of high risk as gold and diamonds are easy to move cross-border (hidden in a car for instance). This modus operandi is closely connected to the assessment of couriers with gold/diamonds (see separate fiche).

Conclusions: the level of ML threat related to purchase of gold and diamonds is considered as very significant (level 4).

Vulnerability

Terrorist financing

The level of TF vulnerabilities related to purchase of gold and diamonds shows that

(a) risk exposure:
Some private sector representatives mention that the use of cash in diamond trade has decreased through the limitations imposed by some national AML legislations (in some cases, payments in cash are limited to 10% of the total amount of the transaction, with a maximum of EUR 3 000). However, there is no specific information coming from the trade in gold where cash payments are still recurrently used with no possibility to identify the parties of the transactions.

(b) risk awareness:
It is very low as far as TF risks are concerned. There is no specific framework in place to limit gold and diamond transportation or purchase. Due to the cross-border characteristic of such movements, controls are difficult/even impossible to implement.
In the case of trade in diamonds, some national organisations of diamond dealers have developed an organisational framework which allows the provision of guidance, trainings and assistance with STRs, as well as some elements contributing to the risk analysis. These organisations may also provide "know your customers" databases which include sanctions lists, PEPs or list of high risk third countries. Some traders in diamonds ensure that identification and verification processes take place before the transaction when the payments are executed through banking transfers.

Nevertheless, these practices remain rather limited and not widespread enough to consider that the sector is well aware about the risks.

For the trade in gold, no specific feedback was received from the private sector as it was impossible to identify a point of contact to discuss AML.

(c) legal framework and controls:
Persons trading in goods are subject to EU AML requirements when they receive payments in cash of EUR 15 000 or more. These AML requirements are limited to payments in cash and do not take into consideration of risks posed by transactions using other means of payment.
As far as trade in diamonds is concerned, one of the largest groups of diamonds in Europe is subject to AML/CFT rules. To that extent, a part of diamonds dealers in the EU are subject to registration requirements (following fit and proper checks – in particular from a BO point of view) and to inspections from their competent authorities that are competent to check both the compliance with AML obligations and cash payments.
The European Union has Kimberley Authorities in 6 European countries that control imported and exported shipments of rough diamonds with focus on the presence of a Kimberley certificate (Belgium, UK, Germany, Czech, Romania and Portugal). This means rough diamonds cannot be imported/exported in/outside the EU without a Kimberley Certificate and without passing through one of the 6 dedicated KP authorities. These 6 KP authorities are appointed by the European Commission and operate under their supervision. So transport of rough diamonds is always subject to controls when entering the EU or when exported. Since trading in rough diamonds without a Kimberly Process certificate equals to 'illegal trade', this is connected to money laundering as an underlying crime and thus Kimberly Process is a strong mitigating measure against money laundering.

The EU framework is rather different for polished diamonds, since they can be imported anywhere in the EU. For Member States who have a very strict import and export control system for diamonds that are imported from countries outside the EU or exported outside the EU, it is possible to circumvent this control mechanism by importing/exporting via a different country of the EU.
However, currently, national legislations in place are not harmonised neither for diamonds nor for gold and this situation generates some risks of discrepancies in the obligations imposed (such as the registration) and the controls applied.
In the case of gold, the lack of harmonised framework is equally problematic from a control and enforceability point of view.
The number of STRs is rather low for this category of obliged entities. Transactions are often face-to-face which poses a specific challenge for protection of employees.

Conclusions: on the basis of the elements above, the level of TF vulnerability related to purchase of gold and diamonds is considered as significant (level 3).

Money laundering

The level of ML vulnerability related to purchase of gold and diamonds shows that

(a) risk exposure:
Some private sector's representatives mention that the use of cash in diamond trade has decreased through the limitations imposed by some national AML legislations (in some cases, payments in cash are limited to 10% of the total amount of the transaction, with a maximum of EUR 3000). However, there is no specific information coming from the trade in gold where cash payments are still recurrently used with no possibility to identify the parties of the transactions.

(b) risk awareness:
It is very low as far as ML risks are concerned. There is no specific framework in place to limit gold and diamond transportation or purchase. Due to the cross-border characteristic of such movements, controls are difficult/even impossible to implement.
In the case of trade in diamonds, some national organisations of diamond dealers have developed an organisational framework which allows the provision of guidance, trainings and assistance with STRs, as well as some elements contributing to the risk analysis. These organisations may also provide "know your customers" databases which include sanctions lists, PEPs or list of high risk third countries. Some traders in diamonds ensure that identification and verification process takes place before the transaction when the payments are executed through banking transfers.

Nevertheless, these practices remain rather limited and not widespread enough to consider that the sector is well aware about the risks. The majority of the diamond or gold sector consists of small companies (often 1-person companies) where the person in charge has no legal background and may find it difficult to put the anti-money laundering legislation in practice and apply CDD procedures.
For the trade in gold, no specific feedback was received from the private sector as it was impossible to identify a point of contact to discuss AML.

(c) legal framework and controls:
Persons trading in goods are subject to EU AML requirements when they receive payments in cash of EUR15 000 or more. These AML requirements are limited to payments in cash

and do not take into consideration of risks posed by transactions using other means of payment.
As far as trade in diamonds is concerned, one of the largest groups of diamonds in Europe is subject to AML/CFT rules. To that extent, some of the diamonds dealers in the EU are subject to registration requirements (following fit and proper checks – in particular from a BO point of view) and to inspections from their competent authorities that are competent to check both the compliance with AML obligations and cash payments.
The European Union has Kimberley Authorities in 6 European countries that control imported and exported shipments of rough diamonds with focus on the presence of a Kimberley certificate (Belgium, UK, Germany, Czech, Romania and Portugal). This means rough diamonds cannot be imported/exported in/outside the EU without a Kimberley Certificate and without passing through one of the 6 dedicated KP authorities. These 6 KP authorities are appointed by the European Commission and operate under their supervision. So transport of rough diamonds is always subject to controls when entering the EU or when exported. Since trading in rough diamonds without a Kimberly Process certificate equals to 'illegal trade', this is connected to money laundering as an underlying crime and thus Kimberly Process is a strong mitigating measure against money laundering.

The EU framework is rather different for polished diamonds, since they can be imported anywhere in the EU. For Member States who have a very strict import and export control system for diamonds that are imported from countries outside the EU or exported outside the EU, it is possible to circumvent this control mechanism by importing/exporting via a different country of the EU.
However, currently, national legislations in place are not harmonised neither for diamonds nor for gold and this situation generates some risks of discrepancies in the obligations imposed (such as the registration) and the controls applied.
In the case of gold, the lack of harmonised framework is equally problematic from a control and enforceability points of view.
The number of STRs is rather low for this category of obliged entities. Transactions are often face-to-face which poses a specific challenge for protection of employees.

Conclusions: even if regulations in place in some Member States have increased the level of risk awareness, the sector is still not well organised enough to allow the implementation of efficient controls and guidance. In that context, the level of ML vulnerability related to purchase of gold and diamonds is considered as significant (level 3).

Mitigating measures

1) For Member States

- Member States should take due consideration of the risks posed by payment in cash in their national risk assessments in order to define appropriate mitigating measures such as the introduction of cash limits for payments, Cash Transaction Reporting systems, or any other measures suitable to address the risk. Member States should consider making sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of their NRA.

- Member States should ensure that competent authorities conduct sufficient unannounced spot checks in diamond companies and traders in gold to identify

possible loopholes in the compliance with CDD requirements and the involvement of check the flow of goods via diamond experts

2) For obliged entities

- Training on CDD, in particular for small businesses.

This role can be taken up by a sector federation or diamond bourse in case of traders in diamond. The training may be about basic AML/CFT requirements such as how to identify, how to perform a risk analyses, what are UBO's, how to notify to the FIU, what is the FIU, etc…

- Promoting the use of written contracts to get a very detailed invoice with a clear description of the goods (value, weight, quality...)

3) For the Commission

- The Commission proposed to amend the definition of cash to include gold in the context of the revision of the Cash Control Regulation (COM(2016) 825);
- Additional studies could be carried out in order to deepen the analysis of economic sectors / situations more exposed to AML/CFT risks.

A further typology work could be carried out to identify economic sectors particularly vulnerable to ML/TF risks before defining tailor made mitigating measures. This analysis could also map Member States practices since many of them have decided to subject certain additional professions to the AML/CFT regime due their risk analysis.

High value assets – other than precious metals and stones

Product

High value assets – other than precious metals and stones

Sector

High value dealers

Description of the risk scenario

Perpetrators use high value goods as an easy way to integrate funds into the legal economy, converting criminal cash into another class of asset which retains its value and may even hold opportunities for capital growth. Certain products such as cars - but also jewellery, watches, luxury boats are particularly attractive as both lifestyle goods and economic assets.

Threat

Terrorist financing

The assessment of the TF threat related to purchase of other kind of high value goods (other than gold, diamonds, artefacts and antiques) has not been considered as relevant from a TF perspective. In that context, the TF threat is not part of this assessment.

Conclusions: non relevant

Money laundering

The assessment of the ML threat related to purchase of other kind of high value goods (other than gold, diamonds, artefacts and antiques) shows that criminal organisations have recurrently used this modus operandi, which is easy to access and do not require specific expertise (trafficking in jewelleries, cars, boats, watches).

Conclusions: the level of ML threat related to purchase of other kind of high value goods is considered as very significant (level 4)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to purchase of other kind of high value goods (other than gold, diamonds, artefacts and antiques) has not been considered as relevant from a TF perspective. In that context, the TF vulnerability is not part of this assessment.

Conclusions: non relevant

Money laundering

The assessment of the ML vulnerability related to purchase of other kind of high value goods (other than gold, diamonds, artefacts and antiques) shows that this risk scenario shares the same vulnerabilities as the one related to purchase of gold/diamonds.

(a) risk exposure:
It is difficult to identify precisely the different kind of goods that may be used to launder money. However; trade on high value goods other than golds and diamonds may rely heavily on cash transactions, with low level of security and monitoring in the delivery channels. It may imply cross-border transactions that are difficult to monitor.

(b) risk awareness:
It is very low as far as ML risks are concerned. The sector is realty wide and there is no particular organisational framework that may allow the provision of guidance or training. Customer due diligence measures are not applied and the level of STR demonstrates that the understanding of the risk is really low.

(c) legal framework and controls:
Persons trading in goods are subject to EU AML requirements when they receive payments in cash in an amount of EUR15 000. However, this definition is rather general and do not specify which category of traders in good fall under the scope of AMLD. In addition, these AML requirements are limited to payments in cash and do not take into consideration of risks posed by transactions using other means of payment. Nevertheless, some Member States have put in place cash payment restrictions.
However, there are no harmonised national legislations in place to address risks posed by high value goods trading. It seems that the level of record keeping is really low and that controls are not applied.

Conclusions: even if regulations in place in some Member States have increased the level of risk awareness, the sector is still not well organised enough to allow the implementation of efficient controls and guidance. In that context, the level of ML vulnerability related to purchase of other kind of high value goods is considered as significant (level 3).

Mitigating measures

1) For the Commission:

- An impact assessment for a possible initiative to swiftly reinforce the EU framework on the prevention of terrorism financing by enhancing transparency of cash payments through an introduction of a restriction of cash payments or by any other appropriate means. By restricting the possibilities to use cash, the proposal would contribute to disrupt the financing of terrorism, as the need to use non anonymous means of payment would either deter the activity or contribute to its easier detection and investigation. Any such proposal would also aim at harmonising restrictions across the Union, thus creating a level playing field for businesses and removing distortions of competition in the internal market. It would additionally foster the fight against money laundering, tax fraud and organised crime.

- Member States should notify the measures applied by dealers in goods covered by the AMLD to comply with their AML/CFT obligations. On this basis, the Commission could further assess risks posed by providers of service accepting cash payments. It will further assess the added value and benefit for making additional sectors subject to AML/CFT rules.

2) For Member States:

- Member States should take due consideration of the risks posed by payment in cash in their national risk assessments in order to define appropriate mitigating measures such as the introduction of cash limits for payments, Cash Transaction Reporting systems, or any other measures suitable to address the risk. Member States should consider making sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of

their NRA.

Couriers in precious metals and stones

Product
Gold and other precious metals
Sector
/
Description of the risk scenario
Cross-border gold and other precious metal movements – as well as precious stones. Perpetrators who generate cash proceeds seek to convert them into gold and other precious metals or stones and move these profits from their source, either to repatriate funds or to move them to locations where one has easier access to placement in the legal economy. Couriers may use air, sea or rail transport to cross an international border: - containerised or other forms of cargo, concealed in mail or post parcels: If perpetrators wish to move very large amounts of gold and other precious metal, often their only option is to conceal it in cargo that can be containerised or otherwise transported across borders. - sophisticated concealments of gold within goods sent by regular mail or post parcel services.
Threat
Terrorist financing The assessment of the TF threat related to gold and other precious metals couriers shows that there are few indicators that terrorist groups use or have the intention to use this channel to finance terrorist activities. Use of gold or diamonds does not constitute the most attractive and secure option for terrorist groups – although these assets are frequent in war zone since they are easy to trade. Some instances of foreign terrorist fighters who have changed their belongings into gold have been detected / reported but the situation is not recurrent and requires, in any case, planning and knowledge. **Conclusions: gold and precious metals couriers do not represent a preferred option for terrorist groups who tend to favour more the use of cash. In that context, the level of TF threat is considered as lowly significant to significant (2)**
Money laundering The assessment of the ML threat related to gold and other precious metals couriers shows that organised crime organisations have exploited this modus operandi to launder proceeds of crime. Unlike terrorist organisations, organised crime groups consider it as an attractive way to launder proceeds of crime. It requires more planning than cash couriers but without the need for major expertise as long as it concerns easy-tradable assets (i.e. preference for gold compared to other precious metals – diamonds compared to other stones). Operations are still at low costs. Hence perpetrators have the needed capacity and intention to use this modus operandi. LEAs report that other types of precious metals have been used (silver, platinum) but these are not frequent because they are less easily tradable and have higher exchange costs than gold/diamond. **Conclusions: the level of ML threat related to gold and other precious metals couriers**

is considered as <u>significant</u> (level 3)

Vulnerability

<u>Terrorist financing</u>

The assessment of the TF vulnerability related to gold and other precious metals couriers shows that

(a) risk exposure
The assessment of the TF vulnerability shows that the risk exposure is intrinsically linked to the cash based activity (anonymity, speediness). Hence the risk exposure is particularly important for this modus operandi.

(b) risk awareness
The sector shows limited awareness to the risks and the controls in place are particularly weak. LEAs have also noticed that criminal organisations use the benefit of the vagueness of the EU framework, in particular as far as cash controls disclosure are concerned.

(c) legal framework and controls
There are no controls in place through the mandatory declaration of transportation of precious metals/stones at the EU external borders (i.e. not covered by the Cash Control Regulation). These assets are not easy to detect. Controls in the countries of destination outside the EU do not allow mitigating the risks (conversion of gold/diamond in cash in country of destination without CDD).

<u>Conclusions</u>: gold and other precious metals couriers are not properly monitored because of the limited awareness of the sector. The controls in place are weak and the reliance on cash increases the vulnerability. There are no controls in place for declaring movement of precious metals/stones at the EU external border. In that context, the level of TF vulnerability related to gold and other precious metals couriers is considered as <u>very significant</u> (level 4).

<u>Money laundering</u>

The assessment of the ML threat related to gold and other precious metals couriers shows that:

(a) risk exposure
The risk exposure is intrinsically linked to the cash based activity (anonymity, speediness). Hence the risk exposure is particularly important for this modus operandi.

(b) risk awareness
The sector shows limited awareness to the risks and the controls in place are particularly weak. LEAs have also noticed that criminal organisations use the benefit of the vagueness of the EU framework, in particular as far as cash controls disclosure are concerned.

(c) Legal framework and controls
There are no controls in place through the mandatory declaration of transportation of

precious metals/stones at the EU external borders (i.e. not covered by the Cash Control Regulation). Those assets are not easy to detect. Controls in the countries of destination outside the EU do not allow mitigating the risks (conversion of gold/diamond in cash in country of destination without CDD).

Conclusions: gold and other precious metals couriers are not properly monitored because of the limited awareness of the sector. The controls in place are weak and the reliance on cash increases the vulnerability. There are no controls in place for declaring movement of precious metals/stones at the EU external border. In that context, the level of ML vulnerability related to gold and other precious metals couriers is considered as very significant (level 4).

Mitigating measures

The Commission will present a legislative proposal revising the cash control Regulation to further mitigate those risks. In order to provide competent authorities with adequate tools, the proposal intends to:

- Enable authorities to act on amounts lower than the declaration threshold of EUR10 000, where there are suspicions of criminal activity;
- Improve the exchange of information between authorities and Member States;
- Enable competent authorities to demand disclosure for cash sent in unaccompanied consignments such as cash sent in postal parcels or freight shipments;
- Extend the definition of 'cash' so as to also include precious commodities acting as highly liquid stores of value such as gold, and to prepaid payment cards which are currently not covered by the standard cash control declaration.

Investment real estate

Product

Investment real estate

Sector

Real estate sector, independent legal professionals, notaries, credit institutions

Description of the risk scenario

Perpetrators are laundering the proceeds of crime in the country by investing in the real estate sector. Perpetrators purchase an asset at below market price, paying the difference to the seller under-the-table in cash. Under or over valuation of property: back-to-back loan which may involve financial institutions or mortgage schemes

Perpetrators may invest, as non-resident, in a country (through visa systems) and develop ML/TF network (including via the complicit legal professionals)

Threat

Terrorist financing

The assessment of the TF threat related to investment in real estate has been considered in conjunction with ML schemes related to investment in real estate in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.

Conclusion: in that context, the assessment of the TF threat related to investment in real estate of activities is considered as very significant (level 4)

Money laundering

The assessment of the ML threat related to investment in real estate has highlighted the recurrent use of real estate sector by organised crime organisations to launder proceed of crime. The real estate sector is mostly used in combination with other sectors, such as TCSPs or legal advice, but presents some threat exposure in itself. Reliance on real estate does not require specific expertise or knowledge, and may be rather financially attractive depending on the services provided.

Conclusions: based on the strong evidence gathered by LEAs identifying real estate as recurrently used in ML schemes and due to the fact that their services may be combined with those provided by other non-financial professionals, the level of TF threat related to real estate is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to investment in real estate has been considered in conjunction with ML schemes related to investment in real estate in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.

Conclusion: in that context, the assessment of the TF vulnerability related to investment in real estate of activities is considered as very significant (level 4)

Money laundering

The assessment of the ML vulnerability related to investment in real estate shows that:

(a) risk exposure

Even if it is a decreasing phenomenon, the use of cash is still possible to finance real estate transactions, which increases the risk of anonymous transactions. More substantially, the risk exposure is increased by the fact that real estate agents are most of the time involved in a business relationship together with other professionals which hinder the effective monitoring of the business relationship (each sector relying on each other to conduct the controls). Real estate activities may be based on financial flows coming from outside the EU and high risk customers, such as PEPs.

(b) risk awareness

The level of awareness is uneven throughout the sector, and depends in particular on the size of the structure concerned. Bigger structures seem more aware of their risks to be misused and consider that they have a role to play in monitoring their customers. They are developing information and training tools, as well as risk assessments. Members of the sector are well aware about their legal obligations, such as cases where increased due diligence is required.

As far as small entities are concerned, this level of awareness is drastically lower because: (i) they are not necessarily integrated in a centralised organisational framework where guidance and training may be delivered; (ii) while they deal with a lower level of sales, they may have difficulty in understanding and applying a complex AML framework (this is the case in particular for single entrepreneurs); (iii) they tend to rely on other sectors to conduct the CDD. This last element tends to be a common feature of the whole sector, where real estate agents may consider that they are the sole responsible for the monitoring of the transactions as other professionals are involved. The same information may not be available at all stages of the transaction (for instance if the identity of the buyer changes for practical or commercial reasons) and this change does not appear at the beginning of the business relationship. The level of awareness of small entities depends on the extent of the training available.

In any case, the "scattering" of obliged entities involved does not simplify the implementation of controls and the understanding of the CDD to be applied. The supervision of the sector is also incomplete and based on weak information trails (no written contracts, solicitors used only to stamp a document).

(c) legal framework and controls in place:

Real estate agents are subject to AML requirements at EU level.

However, it appears that controls in place are not efficient enough. The involvement of several obliged entities in real estate transactions makes it more difficult for competent authorities to identify the role played by a real estate agent and in drawing red flags. On that matter, there are differences between countries as to the legal practices and procedures followed in a real estate transaction. In some countries, the estate agent is able to prepare the preliminary legal documentation (although a legal professional may be required to finalise the transaction), while in other countries, a solicitor prepares the legal documentation including the contract. The level of STRs is uneven, and when it's rather satisfactory, it is due to the reporting of obliged entities other than real estate agents (some real estate agents seem to consider that as they are not involved in the transfer of funds they are not in charge of the STR). The consequence is that investigative authorities may conduct their analysis but not on the basis of the real estate information. It is also important to mention that private sector representatives tend to consider that identification of the beneficial ownership remains an

important challenge as the registration of such information is, at this stage, not mandatory. This is particularly the case when seller and buyer transact in "trust".

<u>Conclusions</u>: the real estate sector is not sufficiently organised to ensure raising a correct level of risk awareness. The involvement of different kinds of obliged entities in a real estate transactions/ business relationships tend to dissuade the sector to conduct its own customer due diligence. The level of STR is not satisfactory; the controls difficult to implement and there is a weak information trail. In that context, the level of ML vulnerability related to real estate sector is considered as <u>significant/very significant (level 3/4).</u>

Mitigating measures

<u>1) for competent authorities</u>

- Member States should ensure that competent authorities/self-regulatory bodies supervising real estate sector produce an annual report on supervisory measures put in place to ensure that the sector accurately apply its AML/CFT obligations. When receiving suspicious transaction reports, self-regulatory bodies shall report annually on the number of reports filed to the FIUs.

- On-site inspections commensurate the population of the real estate representatives in the Member State's territory.

<u>2) for Member States</u>

- Member States should provide guidance on risk factors arising from real estate transactions and specific training to face situations where several professionals are involved in the real estate transaction (estate agent, legal professional, financial institution).

Services from accountants, auditors, tax advisors

Product

services from accountants, auditors, tax advisors

Sector

External accountants, auditors, tax advisors

General description of the sector and related product/activity concerned

Tax advisers perform a range of different professional activities. In the area of tax advice, the main ones could be grouped as follows:

- Tax compliance: Preparation of tax returns, social security and payroll, compliance with various statutory reporting, registration or publication requirements;
- Advisory: Advice on specific tax-related questions that do not occur on a regular basis (e.g. inheritances, mergers or spin-offs, insolvencies, setting up of a company, purchase of immovable property), tax investigation, tax planning / tax optimisation;
- Tax litigation and appeals, advice on these proceedings, representation in criminal tax cases.

The main activities of tax advisers differ from country to country, depending on whether the tax profession is organised more similar to accountants or to lawyers.

In 7/22 countries (BE, ES, GR, IE, PT, RO, SK), tax advisers may not represent their clients before tax (or, where applicable, administrative) courts as this can only be done by lawyers; in Ireland and Spain however tax advisers may represent clients before tribunals in an appeals procedure. In 8 countries (FI, IT, LV, LU, NL, PL, CH, UK), tax advisers may represent their clients before court in fiscal matters but not in criminal tax matters (in Luxembourg, this refers to representation by accountants before the court in first instance). In 6 countries (AT, CZ, DE, HR, RU, UA), tax advisers may also represent their clients in criminal tax matters (although that does not take place in practice in CZ and HR). In 8 countries (AT, DE, FI, LV, NL, PL, RU, UA), tax advisers may represent their clients before the Supreme Court in tax matters while Austria and Finland point out that this applies only to the Supreme Administrative Court. In France, tax advisers are lawyers.

Whether or not tax adviser is a separate profession in a country, few tax advisers practice exclusively in tax. As tax is often related to other areas, it is common that tax advisers provide services in these fields as well (accounting, pension, consulting, legal, advice on company law, audit or arbitration).

At EU level, apart from the Treaty on the Functioning of the EU, a number of European directives have an impact on the tax profession:
- Professional Qualifications (PQ) Directive 2005/36/EC,
- Services Directive (2006/123/EC),
- Directives covering temporary services (1977/249/EEC) and establishment (1998/5/EC) of lawyers
- Directive 2005/60/EC
- Directive 2011/83/EU comes into play where tax advisers have consumer clients
- Directive 2000/31/EC applies to cross-border tax advisory services

No consolidated data on **external accountants and auditors** were provided at the time of the analysis. Statistics presented in Annex 4 give an indication of the size of the sector.

Description of the risk scenario

Perpetrators may employ or require the services of accountants, auditors or tax advisors with a more or less level of involvement of the accountant, auditor or tax advisor himself with the aim to:

- misuse client accounts,

- purchase of real property,

- creation of trusts and companies/ management of trusts and companies,

- undertaking certain litigation, setting up and managing charities

- over or under-invoicing or false declaration around import/export goods.

- providing assurance

- tax compliance

They may be involved in ML schemes through the creation of 'opaque structures' defined as business structures where the true identity of the owner(s) of entities and arrangements in that structure is concealed through the use of, for example, nominee directors. The creation of such structure often set up in multiple jurisdictions including offshore centres is complicated and requires both regulatory and tax services of professionals.

Threat

Terrorist financing

The assessment of the TF threat related to services from accountants, auditors, tax advisors has been considered in conjunction with ML schemes related to services from accountants, auditors, tax advisors in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.

Conclusion: in that context, the assessment of the TF threat related to services from accountants, auditors and tax advisors is considered as very significant (level 4)

Money laundering

The assessment of the ML threat related to services from accountants, auditors and tax advisors presents some commonalities with legal advice from legal professionals.

- as it is the case for all other legal activities**, risk of infiltration or ownership by organised crime group**s is a ML threat for accountants, auditors and tax advisors. These professionals may be unwittingly involved in the money laundering but may be also complicit or wilfully negligent in conducting their customer due diligence obligations.

- LEAs have evidence that organised crime organisations recurrently used tax advisors advice and seek out the involvement of this sector in their ML schemes. The reliance on tax advisors services is considered as a viable means to put in place ML schemes either because the involvement of this professional is needed to carry out certain type of activities or because access to specialised tax expertise and skills may assist the laundering of the proceeds of crime. Access to tax advisors legal services is quite easy and does not require specific competences or expertise in itself. As far as the setting up of the ML scheme is concerned, criminal organisations rely on these professions' skills which allow them not to develop these competences themselves. In addition, there is evidence that some criminals seek to co-opt and knowingly involve tax advisors in their money laundering schemes. Often however the involvement of tax advisors is sought because the services they offer are essential to the specific transaction being undertaken and they add respectability to the transaction.

Conclusions: Services from tax advisors/auditors/accountants are recurrently used in ML schemes, are considered as easily accessible and seen by organised crime organisations as a way to compensate their lack of expertise.

In that context, the level of ML threat related to services from accountants, auditors and tax advisors is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to services from accountants, auditors, tax advisors has been considered in conjunction with ML schemes related to services from accountants, auditors, tax advisors in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.

Conclusions: in that context, the assessment of the TF vulnerability related to services from accountants, auditors and tax advisors is considered as significant (level 3) similar to ML

Money laundering

The assessment of the ML vulnerability related to services from accountants, auditors and tax advisors shows that

(a) risk exposure of this sector is impacted by the fact that this sector could be quite often involved in the management of complex transactions involving tax related advice. These transactions may expose the sector to customers who may present high risk features (such as politically exposed persons for instance) or to complex legal entities or legal arrangements where the identification of the beneficial owner is particularly challenging. At the same time, this sector presents high ability to manage tax matters related to these complex legal entities and legal arrangements, as they constitute their core business.

(b) risk awareness:
Accountants, auditors and tax advisors are required to adhere to strict ethical or professional rules. They tend to consider that this should therefore be a sufficient deterrent to ML and TF occurring in or through their sector. It is nevertheless worth noting that this sector may also be infiltrated by organised crime organisation and that the supervisory bodies are not still well equipped to detect this kind of abuse (i.e. lack of fit and proper test requirement).

This sector benefits from a strong organisation framework at EU level. For instance, the Confédération Fiscale Européenne (CFE) embraces 26 national organisations from 21 European States, representing more than 200 000 tax adviser. Accountancy Europe unites 50 professional organisations from 37 countries that represent close to 1 million professional accountants, auditors, and advisors. The role of these organisations is to ensure exchange of information about national laws relevant to their sector and to co-ordinate respectively on EU legislation. It is nevertheless not always a guarantee of high quality cooperation with competent authorities. In addition, competent authorities and FIUs tend to consider that accountants, auditors and tax advisors are still not aware enough about the risks posed by opaque structures and mechanisms that are put in place to obscure the beneficial ownership.
(c) legal framework and controls
Accountants, auditors and tax advisors are subject to the EU anti-money laundering requirements since 2001. They shall apply customer due diligence where they participate,

whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts; (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies, foundations, or similar structures.

Tax advisors, accountants and auditors represent a quite complex and diverse professional sector. Generally speaking, it is characterised by long-term business relationships which increase ability of professionals to detect unusual transactions or behaviour. Nevertheless, other activities which relate to one specific tax advice on a related transaction, that occur only once or at irregular intervals may lead the professional to fulfil its task without having a full understanding of his customer's financial situation. This variety has an impact on the level of the reporting that is better than lawyers, whilst still rather low. This low level of STRs is sometimes justified by the sector by the fact that, in this field, the professional in charge does not process or initiate a financial transaction on his customer's behalf. Red flags are not based on the transaction but on any unusual patterns of behaviour. Some of the work of accountants and tax advisors may include an element of investigation and auditing that may constitute useful intelligence for possible STRs.

Given that opaque structures can be created through many jurisdictions, including offshore centres, professionals avail of an opportunity to take advantage of tax and regulatory differences to sell professional services.

Conclusions: accountants, auditors and tax advisors are better organised than other legal professionals. However, they suffer from the same weaknesses as far as the controls and the management of the risks (BO in particular) are concerned. In that context, the level of ML vulnerability related to services from accountants, auditors and tax advisors is considered as significant (level 3).

Mitigating measures

1) for the Commission

- in the context of Directive (EU) 2015/849:

- transposition checks on the implementation of transparency requirements for beneficial ownership information (registration): Member States should notify technical elements of their national AML/CFT regime ensuring transparency requirements for beneficial ownership information;
- transposition checks on the implementation of identification requirements for beneficial ownership information (definition of the beneficial owner): Member States should notify technical elements of their AML/CFT regime related to beneficial owner definition

- in the context of Commission's proposal COM(2016)450: reinforcing the transparency requirements for beneficial ownership information on legal entities and legal arrangements

2) for competent authorities

- Member States should ensure that competent authorities/self-regulatory bodies supervising auditors, external accountants and tax advisors produce an annual report on supervisory measures put in place to ensure that the sector accurately apply its AML/CFT obligations. When receiving suspicious transaction reports, self-

regulatory bodies shall report annually on the number of reports filed to the FIUs.

- On-site inspections commensurate to the population of auditors, external accountants and tax advisors representatives in the Member State's territory.

3) for Member States

- Member States should provide guidance on risk factors arising from transactions involving auditors, external accountants and tax advisors.

- Promote a better understanding for interpreting and applying the legal privilege by auditors, external accountants and tax advisors. Member States should issue guidance on implementation of the legal privilege**:** how to split between legal services subject to the very essence of legal privilege and other legal services not subject to legal privilege when provided to a same client. .

Legal service from notaries and other independent legal professionals

Product

Legal service from legal professionals

Sector

Independent legal professionals, lawyers, notaries

Description of the risk scenario

Perpetrators may employ or require the services of a legal professional (such as lawyers, notaries and other independent legal professions) with a more or less level of involvement of the legal professional himself:

- misuse of client accounts,

- purchase of real property,

- creation of trusts and companies/ management of trusts and companies,

- undertaking certain litigation

They may be involved in ML schemes through the creation of 'opaque structures' defined as business structures where the real identity of the owner(s) of entities and arrangements in that structure is concealed through the use of, for example, nominee directors. The creation of such structures often set up in multiple jurisdictions including offshore centres is complicated and requires both regulatory and tax services of professionals.

Threat

Terrorist financing

The assessment of the TF threat related to legal service from legal professionals has been considered in conjunction with ML schemes related to legal service from legal professionals in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.

Conclusion: in that context, the assessment of the TF threat related to services from legal professionals is considered as very significant (level 4)

Money laundering

The assessment of the ML threat related to legal services from legal professionals presents some commonalities with legal services from accountants, auditors and tax advisors.

- as it is the case for all other legal activities, risk of infiltration or ownership by organised criminal groups is a ML threat for accountants, auditors and tax advisors. These professionals may be unwittingly involved in the money laundering but may be also complicit or wilfully negligent in conducting their customer due diligence obligations.

- LEAs reported that organised crime organisations recurrently used legal services from legal professionals and seek out the involvement of this sector in their ML schemes. The reliance on legal professionals is considered as a viable means to put in place ML schemes either because the involvement of a legal professional is required to carry out certain type of activities or because access to specialised legal and notarial skills and services may assist the

laundering of the proceeds of crime. In the case of lawyers in particular, they are exposed to misuse by criminals because engaging a lawyer adds respectability and an appearance of legitimacy to any activities being undertaken, while providing services which are methods that criminals can use to facilitate money laundering.

Access to legal professionals is not considered as particularly complex to criminal organisations. For criminal organisations, relying on legal professions' skills is a way to avoid developing these competences themselves.

Conclusions: according to LEA information, legal professionals are recurrently used in ML schemes. They are considered as easily accessible and the reliance on legal professionals allow organised criminal organisations to limit their expertise or knowledge's needs, and to bring a "stamp approval" to their actions. In that context, the level of ML threat related to legal professionals (lawyers, notaries and other independent legal professionals) is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to legal service from legal professionals has been considered in conjunction with ML schemes related to legal service from legal professionals in order to hide the illegal origin of the funds. In that context, the TF threat does not benefit from a separate assessment.

Conclusion: in that context, the assessment of the TF threat related to services from legal professionals is considered as significant (level 3)

Money laundering

The assessment of the ML vulnerability related to legal advice from legal professionals shows that:

(a) risk exposure:
The risk exposure of this sector is affected by the fact that it could be quite often involved in the management of complex legal situations. In particular, the fact that legal services do not necessarily lead to handling proper financial transactions requires from legal professionals to trigger other kind of red flags that are more difficult to define (customer's behaviour).

(b) risk awareness:
The sector is not homogeneously organised (scope of legal professionals varies from one Member State to another) even though some EU organisations exist and play an important role in providing information on the application of AML/CFT requirements, in providing guidance and facilitating the exchange of information. They help in particular in setting up a list of red flags that members of the sector can use: client's behaviour or identity, concealment techniques (use of intermediaries, avoidance of personal contact), size of funds (disproportionate amount of private funding). The profession seems to be aware of some risks such as when the customer gives instruction from a distance about transactions, without legitimate reason or when there is a change in legal advisor a number of times within a short space of time or engagement of multiple legal advisers without good reasons.
In general, the level of STR reporting is very low when dealing with legal professionals. According to FIUs, this is much more the case when legal professionals rely on self-

regulatory bodies (SRBs), as allowed under the EU AML framework. Indeed according to the EU AML framework, these SRBs shall forward the suspicious transactions reports to the FIU "promptly and unfiltered". Based on the information provided by the private sector, the reliance on SRBs is required by 6 Member States national laws (Belgium, Czech Republic, France, Germany, Greece, Luxembourg) while for 19 other Member States the law does not require that STRs should be sent to the SRB instead of the FIU (Austria, Cyprus, Estonia, Finland, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom). In Denmark, the reliance on an SRB is left to the lawyer's discretion who can ask the bar for advice/an opinion before reporting to the FIU. If the lawyer decides to ask the bar for advice, the lawyer should not contact the FIU until the bar has provided its opinion on whether or not to bring the case forward to the FIU. FIUs reported that when provided by national laws or used by lawyers on their own decision, these SRBs may act as "filters" of the STR which led to a very low level of reporting (if at all). The quality of the supervision of the sector is also considered as too weak, due to differences in the organisation of the sector at national level.

(**c) legal framework and controls**

Notaries, lawyers and other independent legal professionals are subject to the EU anti-money laundering requirements since 2001. They shall apply customer due diligence where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the (i) buying and selling of real property or business entities; (ii) managing of client money, securities or other assets; (iii) opening or management of bank, savings or securities accounts; (iv) organisation of contributions necessary for the creation, operation or management of companies; (v) creation, operation or management of trusts, companies, foundations, or similar structures.

Legal professionals are organised and regulated in different ways depending on the Member States concerned. In addition, regulators and FIUs consider that the level of controls applied by legal professions' competent authorities is too weak. Legal services are also often carried out face-to-face which present a specific challenge for the protection of employees.

The legal privilege is a recognised principle at EU level which reflects a delicate balance in light of the European Court of Justice ECJ case law on the right to a fair trial (C-305/05), itself reflecting the principles of the European Court of Human Rights as well as of the Charter (such as article 47). At the same time, there are cases where these professionals sometimes conduct activities that are covered by the legal privilege (i.e. ascertaining the legal position of their client or defending or representing their client in judicial proceedings) and at the same time activities that are not covered by the legal privilege, such as providing legal advice in the context of the creation, operation or management of companies. It appears that in such situations, sometimes legal professionals might treat all these activities as captured by the legal privilege principle which might lead to the non-compliance with AML/CFT obligations for parts of the activities. The remit of confidentiality, legal professional privilege and professional secrecy varies from one country to another, and the practical basis on which this protection can be overridden is not always clear or easily understood. This may hinder (i) the STR requirement and related investigative actions (while legal professionals may cease to act but not make an STR when legal professional privilege or professional secrecy applies), and (ii) the exchange of information between FIUs. This aspect of the legal professionals' activity is particularly important, as it may increase criminal organisations' perception that legal privilege is designed to protect them. It also plays a role in the weaknesses identified in that sector to identify red flags in particular as far as beneficial ownership identification is concerned.

<u>Conclusions</u>: risk awareness of the sector is limited due to the organisational framework and the interpretation/scope of the legal privilege principle. Despite a legal framework in place, the number of STRs is still very low and the supervision of the sector does not ensure a proper monitoring of the possible ML abuses. In that context, the level of ML vulnerability related to legal advice from legal professionals is considered as <u>significant</u> (level 3).

Mitigating measures

<u>1) for the Commission</u>

- in the context of Directive (EU) 2015/849:

- transposition checks on the implementation of transparency requirements for beneficial ownership information (registration): Member States should notify technical elements of their national AML/CFT regime ensuring transparency requirements for beneficial ownership information;
- transposition checks on the implementation of identification requirements for beneficial ownership information (definition of the beneficial owner): Member States should notify technical elements of their AML/CFT regime related to beneficial owner definition

- in the context of Commission's proposal COM(2016)450: reinforcing the transparency requirements for beneficial ownership information on legal entities and legal arrangements

<u>2) for competent authorities</u>

- Member States should ensure that competent authorities/self-regulatory bodies supervising independent legal professionals, lawyers, notaries produce an annual report on supervisory measures put in place to ensure that the sector accurately apply its AML/CFT obligations. When receiving suspicious transaction reports, self-regulatory bodies shall report annually on the number of reports filed to the FIUs.

- On-site inspections commensurate to the population of independent legal professionals, lawyers, notaries representatives in the Member State's territory

<u>3) for Member States</u>

- Member States should provide guidance on risk factors arising from transactions involving independent legal professionals, lawyers, notaries.

- Promote a better understanding for interpreting and applying the legal privilege by notaries and independent legal professionals. Member States should issue guidance on implementation of the legal privilege**:** how to split between legal services subject to the very essence of legal privilege and other legal services not subject to legal privilege when provided to a same client..
- Self-regulatory bodies should make efforts to increase the number of thematic inspections and reporting. They should also organise training to develop a better understanding of the risks and AML/CFT compliance obligations.

Gambling sector products

General description of the gambling sector

General description of the sector and related product/activity concerned
The 4th Anti-Money Laundering Directive ("4AMLD") defines a gambling service as a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill, such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services. The term "gambling" thus refers to a range of different services and distribution channels. For the purpose of this risk assessment, the gambling sector has been split into land-based (offline) and online gambling, with the land-based sector further divided into betting, bingo, casinos, gaming machines, lotteries and poker. A further division into different online gambling products has not been considered necessary, at this stage, for this purpose as the relevant risks, threats and vulnerabilities appear to be primarily linked to the nature of online transactions generally rather than to specific forms of online gambling. There is no sector-specific EU legislation on gambling; Member States are free to set the objectives of their policy and to define the level of protection sought for the purpose of protecting consumers and preventing criminality, including money laundering. However, the provisions of the EU Treaty apply. The Court of Justice of the European Union has provided general guidance on the interpretation of the fundamental internal market freedoms in the area of gambling, taking into account its specific nature. While Member States may restrict or limit the cross-border supply of gambling services on the basis of public interest objectives that they seek to protect, they are required to demonstrate the necessity and suitability of the measures in question and that they are being pursued in a consistent and systematic manner. The gambling sector in the EU is thus highly diverse, ranging from monopolistic regimes (run by a state-controlled public operator or by a private operator on the basis of an exclusive right) to licensing systems, or a mix thereof. In response to the societal, technological and regulatory challenges and developments, a significant number of Member States has and/or are in the process of reviewing their gambling legislation taking into account new forms of gambling services, which has led to an increase in the offer of gambling services by operators authorised in an EU Member States as well as cross-border offers not authorised under national rules in the recipient Member State. The gambling sector is characterised by fast economic growth and technological development. For example, online gambling revenues in the EU were estimated at around EUR 16.5 billion in 2015, and expected to rise to around EUR 25 billion by 2020. The revenue of the offline/land-based gambling market is equally expected to increase from around EUR 77.5 billion in 2015 to around EUR 82-84 billion in 2020. Through non-legislative actions, pursuant to the 2012 Communication “Towards a comprehensive European framework for online gambling” (COM (2012) 596 final), the Commission has encouraged Member States to provide a high level of protection, in particular in the light of evidence concerning risks associated with gambling that include the development of addictive disorders and other negative personal and social consequences. In particular, in a Recommendation on the principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online (2014/478/EU), the Commission sets out practices aimed at limiting social harm, some of which may be relevant for anti-money laundering purposes, for example registration and verification processes.

In addition, effective supervision is necessary for the appropriate protection of public interest objectives. Member States should designate competent authorities and lay down clear guidance for operators, also in view of anti-money laundering. The Commission's Expert Group on Gambling Services brings together gambling regulators from all EEA jurisdictions for regular meetings which offer the opportunity to discuss common challenges and exchanges best practices, which, for example, has resulted in a Cooperation Arrangement between the gambling regulatory authorities of the EEA Member States concerning online gambling services (signed by most Member States in 2015).

Controlling the growing, so-called, unauthorised gambling offer and channelling unauthorised gambling offers into the authorised, regulated gambling sector are some of the most important and challenging tasks for regulators across the EU. Across the EU, millions of consumers are estimated to gamble on unauthorised online gambling sites. In connection to this, it is also necessary to create awareness about the inherent risks of unregulated gambling websites, such as fraud, that are outside any form of control at the level of the Union. The extent of such unauthorised, usually online, offers, vary considerably from Member State depending to a large extent the well-functioning of the authorised market.

The unauthorised market, risks and control thereof is outside the scope of this exercise, based on the assumption that it is not possible to directly launder money through an illegal activity (winnings would remain illegal). However, regulators and obliged entities should be aware of online techniques which may make it possible to disguise the true identity of users and sources of money while creating the appearance of legitimate transactions and thus allowing the money to be used in future transactions in legal markets.

Application of 4AMLD

Following the requirements of AMLD4, the whole gambling sector service providers are subject to AML/CFT requirements at the stage of the collection of winning, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

However, with the exception of casinos, Member States may decide – in proven low-risk circumstances - to exempt certain gambling services from the AMLD4 requirements. The use of an exemption by a Member State should be considered only in strictly limited and justified circumstances. Such exemption should be subject to a specific risk assessment, including the nature and scale of operations of such services and the degree of vulnerability of applicable transactions, and shall be notified to the Commission together with a justification based on the specific risk assessment. In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission in the framework of the supranational risk assessment.

Betting

Product
Betting (land-based/offline)
Sector
Gambling sector
General description of the sector and related product/activity concerned
Offline, or land-based, betting services (including horse and dog racing, event betting) offered in dedicated authorised outlets, by authorised retailers (who receive a commission on each bet but also offer other services) or in areas where sport events take place (often horse or dog race tracks). The amount of the prize can either depend on the total amount of the pre-paid stakes (i.e. the so-called "totalisator systems", *pari mutuel* or "pool betting") or on the stake-winnings ratio that is agreed between the bookmaker and the player (i.e. *pari à la cote* or "fixed-odds betting"). The number of service providers that can offer betting services in a Member State may be fixed (including to a single monopoly provider) or open to a non-restricted number of operators that meet certain criteria. Minimum and/or maximum numbers of retail outlets per licenced provider can also be defined.
Description of the risk scenario
Three basic scenarios have been identified: (1) a perpetrator places a bet and cashes in the winnings (conversion); (2) a perpetrator deposits cash into their betting account and withdraws it after a period of time without actually staking it (concealment); (3) a perpetrator places money in a betting account in one location and an accomplice withdraws the funds in another location (concealment, disguise and transfer). A perpetrator can increase their odds of winning by placing bets on a series of events which will give more favourable accumulated odds -or reduce the risk of losing by hedging bets (i.e. betting on both possible outcomes of the same event). A perpetrator can also remove any uncertainty altogether by approaching a winner and purchasing the winning betting slip.
Threat
Terrorist financing The assessment of the TF threat related to betting activities has not been considered as relevant. In that context, the TF threat is not part of the assessment. **Conclusions: not relevant**

Money laundering

The assessment of the ML threat related to betting activities shows that:

- as it is the case for all other gambling activities, one of the ML threats related to betting activities is **the risk of infiltration or ownership by organised crime groups**.

The level of threat related to the risk of infiltration may vary depending on the structure where the betting activities occur. In the case of national sport betting monopolies, the risk of infiltrating the ownership of the sport betting operator itself is close to inexistent. However, it is possible that individual retailers on which they rely to sell their betting services to end customers could be infiltrated.

The infiltration by organised crime organisations in betting activities requires moderate levels of planning or technical expertise, and relies mostly on mechanisms allowing concealing the identity of the beneficial owner, such as the registration of assets under the name of third parties (frontmen).

- another recurring threat is **match-fixing**. Investigations have shown that criminal groups use betting (to profit from fixing sport competitions in the EU). Agents and intermediaries corrupt or intimidate players and/or referees to guarantee their desired outcome in a match, while agents place huge amounts of money betting online, or offline, outside the EU. In such case, match fixing requires contacts (and normally money transfers) between gamblers, players, team officials, and/or referees. A related threat is betting on fictitious matches, or events, although this is rather linked to online betting.

- finally, purchasing of **winning tickets** to ensure winnings may represent another criminal groups intent to launder money.

Conclusion: **Law enforcement authorities have identified several modi operandi that may be used by organised crime groups when dealing with betting activities. Beyond the horizontal threat which is the risk of infiltration and ownership, the other important aspect is match-fixing. The intent and capabilities of organised crime groups to use these modi operandi require moderate levels of planning, knowledge and expertise, given that they are perceived as rather attractive and secure to achieve a financially viable option.**

In that context, the level of ML threat related to betting activities is considered as significant (level 3)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to betting activities has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

The assessment of the ML vulnerability related to betting activities shows:

(a) risk exposure:
Betting activities are characterised by significant volumes of speedy and anonymous transactions, frequently cash based. While the use of cash is reducing due to alternative betting methods, it still represents more than 50% of turnover in some countries. Cash is used essentially for confidentiality or reputational reasons by many bettors.

According to industry experts, possible red flags are bets accepted with large stakes at extremely short odds which are likely to guarantee a return; customers regularly requesting copies of winning bets or receipts of winning tickets; customers paying in cash and regularly requesting winnings to be paid via cheque or by debit card; customers regularly requesting receipts when collecting machine winnings.

(b) risk awareness:

- according to the FIUs the betting sector is not sufficiently aware of the risks as demonstrated by a low level of STRs, as well as their poor quality.

- vulnerability to ML risks is significantly increased by the reliance on distribution networks (kiosks, retailers, points of sale) which are not necessarily submitted to AML/CFT requirements. The identification of the customer is under the responsibility of individual retailers working for the betting operator who may not always have the possibility to detect suspicious transactions (e.g. cumulative bets, division of high bets or unusual bets), depending on how relationships between operators and retailers are organised. The level of STRs is uneven and part of the sector is still not well aware about the risks and/or what types of transactions to report (no consistent reporting obligations).

- according to representatives of the betting sector, there are wrong perceptions and lack of understanding from FIUs and other competent authorities about the risk factors inherent to betting. It seems that FIUs have some a priori on the type of suspicions a gambling operator shall report (FIUs expect suspicious cases of match-fixing while the operator tends to report anomalous amounts in the transaction). Betting operators are suffering from a lack of feedback from FIUs about the STRs.
In addition, betting operators are developing CDD requirements that could mitigate the risks of ML. Even in absence of national requirements to do so, some betting operators are imposing systematic identification of winners (over a certain amount), focusing on the beneficial owner for instance. They could also offer payment methods to limit the use of cash and deploy players' cards to increase operator's knowledge of its customers.

(c) legal framework and controls:
Betting activities are not covered by the current EU AML framework (3AMLD). However, based on its minimum harmonisation principles, some Member States have already extended their national AML/CFT regimes to betting . This has created discrepancies from one Member State to another in terms of regulation, supervision of the sector and enforcement of AML/CFT rules.

Despite the absence of EU legal requirements, certain Member States have already put in place legislation covering ML aspects of betting, and/or specific requirements in licensing agreements. When this is the case, regulations in place tend to be strict both at the level of the

granting of an authorisation (fit and proper AML check of key personnel) and at the level of ongoing reporting obligations. These reporting obligations shall occur each time there are any concerns in relation to the customer, such as knowing whether the staking and loss levels are a cause for concern relating to AML/CFT or whether the customer gambling's habits are consistent with his lifestyle). This implies an effective internal reporting process and a good AML knowledge both from the management and the staff. In that respect, some national legislation requires from the betting sector to conduct a sectorial risk assessment showing that suitable controls and procedures are in place.

However, although some rules are already in place in certain Member States, competent authorities still have concerns about the enforceability of the controls, in particular the monitoring of the bets to detect ML risks in real time and the possibility to suspend the bets in case of suspicion. Given the nature of betting activities (including high-volume or sometimes last- minute betting), it appears challenging to put in place an accurate CDD regime and this needs to be addressed. The reliance on retailers presents an additional level of uncertainty in terms of CDD, considering that some points of sale are not exclusively dedicated to betting and do not have the possibilities and the means to operate such controls (knowing that betting could occur in bars, restaurants, supermarkets, book-shops or gas stations).

Conclusion:

Betting activities do not represent a homogeneous business model, nor are they covered by coherent AML/CFT rules at national level. From a vulnerability assessment point of view, the lack of harmonised AML/CFT regime plays an important role. While it is undeniable that nationally, some betting operators are well aware about their ML/TF risks and their corresponding obligations, it is still uncertain whether they are able to put in place accurate and comprehensive controls due to the characteristics of betting activities (significant volumes of speedy and anonymous transactions, often cash based). Current legislation or rules set out in licence conditions could be improved to better ensure sufficient controls, although the vulnerability assessment shows that risk awareness seems to have increased within betting operators which have started developing some mitigating measures (such as systematic controls above a threshold or alternative payment tools to limit the use of cash).

The apparent lack of understanding by competent authorities and FIUs on the functioning of the betting activities is another obstacle to good AML/CFT risk assessment and guidance. The low level of feedback from FIUs constitutes also a weakness in the mitigation of AML/CFT risks.

In that context, the level of ML vulnerabilities related to betting activities is considered as significant (level 3).

Mitigating measures

1) For competent authorities

- Member States should improve cooperation between relevant authorities (FIUs, LEAs, police, sectorial regulatory bodies such as gambling regulators) to better understand the risks factors inherent to betting activities and to be able to provide efficient guidance.
- Member States should ensure a regular cooperation between relevant authorities and

betting operators. This better cooperation will focus on:
- strengthening the detection of suspicious transactions and to increase the number and the quality of the STRs;
- organising training sessions of the staff and compliance officers, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- provision by supervisory authorities of clearer guidance on AML/CFT risks, on CDD and on STR requirements and how to identify the most relevant indicators to detect money laundering risks;
- ensuring that FIUs provide feedback to betting operators about the quality of the STR, ways to improve the reporting and about the use made of the information provided in, preferably within a set period of time;
- developing standardised STR/SAR template(s) at EU level taking into account specificities of gambling sector

2) For the sector

- Member States should ensure that betting operators organise training sessions of the staff, compliance officers and retailers on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- Member States should ensure that betting operators promote player's cards, or use of electronic identification schemes, to facilitate the identification of the customer and to limit the use of cash, and real-time monitoring systems to identify suspicious transactions at point of sales;
- Member States should ensure that betting operators designate an AML officer at the premises when it is not already the case
- Member States should ensure that betting operators promote systematic risk-based CDD of the winners, and promote a lower threshold of winnings subject to CDD (currently at EUR 2000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission

The Commission should provide guidance on Article 11(d) concerning the implementation of CDD in case of "several operations which appear to be linked".

Bingo

Product
Bingo (land-based/offline)
Sector
Gambling sector
General description of the sector and related product/activity concerned
Offline or land-based, bingo is a game of chance, in which the player uses a scorecard or an electronic representation thereof bearing numbers and is played by marking or covering numbers identical to numbers drawn by chance, whether manually or electronically, and won by the player who first marks or covers the "line" which is achieved when, during one game, for the first time all five numbers on one horizontal row on one scorecard are drawn; or the "house" or "bingo" is achieved when, during one game, for the first time all the numbers on one scorecard are drawn. Prizes may be given in kind (vouchers), paid immediately at the gambling venue, or given as cash prizes. They can also consist in household items, novelty items or food. In some Member States, limited money prizes are nevertheless possible and in other Member States, nothing prevents providers of bingo services from offering purely cash prizes. Bingo is primarily a locally based, SME-driven activity which rarely transcends national borders. While in most Member States bingo is considered a game of chance, in many others it is considered a form of lottery.
Description of the risk scenario
A perpetrator purchases cards - traditionally with cash - on which a random series of numbers are printed. Players mark off numbers on their cards which are randomly drawn by a caller (employed by the gambling operator), the winner being the first person to mark off all their numbers. A winning card could be purchased for a higher amount, like a lottery ticket or betting slip.
Threat
Terrorist financing The assessment of the TF threat related to bingo has not been considered as relevant. In that context, the TF threat is not part of the assessment. **Conclusions: not relevant**
Money laundering The assessment of the ML threat related to bingo shows that: - as it is the case for all other gambling activities, one of the ML threat related to bingo activities is **the risk of infiltration or ownership by organised crime groups**. The level of threat related to the risk of infiltration may vary depending on the structure where bingo activities occur. In case of bingo, it appears that infiltration occurs when street criminals run bars where bingo draws are not controlled and may be used for ML purposes (make the funds licit while coming from illegitimate origin). - except the risk of infiltration, this risk scenario is rarely used by criminals to launder proceed of crime due to the fact that it is financially not very attractive as amounts at stake are quite small and outcome insecure (drawings based on chance).

Conclusions:

Beyond the horizontal threat which is the risk of infiltration and ownership, bingo is not considered by LEAs and other competent authorities as an attractive scenario to launder proceeds of crime. The chance component of bingo makes it rather unattractive and highly insecure. There are few indicators that criminals have the capabilities and intent to use it, and in any case, it would likely be for very low amounts of winning.

In that context, the level of ML threat related to bingo is considered as lowly significant (level 1).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to bingo has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML vulnerability related to bingo shows:

(a) risk exposure:
The scale of bingo's activities is rather limited and represents a low level of financial transactions. When played offline, the activity is mostly cash based. It relies on relatively low stakes and winnings, with prices often in kind. It involves no or very low level of high risk customers and/or high risk areas.

(b) risk awareness :
Considering the absence of cases where bingo has been used to launder proceeds of crime, this component is difficult to assess. Equally, it has not been possible to determine if the lack of ML cases is due to the high level of awareness of ML risks or rather to the low level of intent of criminal organisations to use this scenario.

(c) legal framework and controls:
Bingo activities are not covered by the current EU AML framework (3AMLD). However, based on minimum harmonisation principles of it, some Member States have already extended their national AML/CFT regimes to bingo. This has created discrepancies from one Member State to another in term of regulation, supervision of the sector and enforcement of AML/CFT rules.
In the case of bingo, this gambling activity does not exist in all Member States, but where it exists, it should be subject to AML regulation. At national level, bingo operators may either be covered under the regulation of casinos or they may benefit from a specific regulation (e.g. football club owning its own bingo house). Representatives of the bingo sector have mentioned that thresholds are put in place for systematic identification, which has been confirmed by competent authorities which tend to confirm that controls are in place and that they are rather efficient. Once again, the relatively low levels of amounts at stake and/or winnings play a role in the overall vulnerability assessment.

Conclusion: The characteristics of bingo makes it lowly vulnerable to ML risks. It is largely based on chance, with fairly low stakes and winnings (often in kind). Although

mainly cash based, this activity does not involve particularly high amounts of stakes. In countries with bingo activities, it should be subject to AML/CFT rules with controls in place which seem rather efficient and satisfactory. It should be noted that the risk awareness component was not possible to assess properly due to the lack of reported cases. In that context, the level of the ML vulnerability is considered as <u>lowly significant</u> (level 1).

Mitigating measures

Member States should ensure that bingo operators organise training sessions of the staff and compliance officers on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly. In view of this they should also continue monitoring bingo activities to identify possibly future risks.

Casinos

Product

Casino (land-based/offline)

Sector

Gambling sector

General description of the sector and related product/activity concerned

In several countries (Belgium, the Czech Republic, France, Luxembourg, Portugal and Slovakia), a casino (offline/physical establishment) is defined as a place where games of chance are organised (whether automatic or not) and where other cultural and social activities (theatre, restaurants) take place. In other countries (Austria, Denmark, Estonia, Finland, Germany, Latvia, Malta, the Netherlands and Sweden), it is not necessary that the casino manages other social or cultural activities, whereas some Member States (Denmark, Finland, Ireland and the United Kingdom) have not directly defined the concept of casino gaming.

Casinos may be state or privately owned and in some Member States, only a single operator is licensed (Finland, Austria, the Netherlands and Sweden).

Casinos are the only gambling services covered by EU AML legislation (Directive 2005/60/EC - 3rd Anti-Money Laundering Directive).

Description of the risk scenario

A perpetrator purchases chips at the casino at a dedicated point of sale (for cash or anonymous pre-paid cards) and these chips can be used when playing on a wide variety of games (with clearly defined rules). Casino staff (croupiers) interacts with players in well regulated games such as Baccarat roulette, black-jack and many more. If winning, the player receive chips at the table, which then have to be converted back to cash at a dedicated point of sale (whereby legitimising illicit funds).

A perpetrator could use 'mules' or collaborators that buy chips on his behalf for illicit cash and the main perpetrator will receive the chips in the casino – and exchanging the chips to cash pretending that he won these in the games offered at the casino.

A perpetrator could also take advantages from the fact that certain casino games provide for a high return on stakes (depending on high/low risk bets). Two players may also cooperate and place bets on a roulette table on red and black at the same time with only a 3% chance of losing their accumulated stakes.

A perpetrator may also transfers funds from one casino to another (if legally allowed), giving access to chips to another player. In such cases, casinos are used like financial institutions through accounts to accounts transfers of funds.

Threat

Terrorist financing

The assessment of the TF threat related to casinos has not been considered as particularly relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of ML threat related to casinos shows that, as it is the case for all other gambling activities, one of the ML threat related to casinos is **the risk of infiltration or ownership by organised crime groups**. In the case of casinos, LEAs have particularly indicated that casinos would be exposed to infiltration threats. However, casinos which are under State monopolies or public companies appear to be less exposed to infiltration threats, due to regulations in place imposing for example transparency on beneficial ownership. This element may have an impact on the intent and capability of organised crime groups to infiltrate casinos. Stakeholders have also pointed out that national licensing systems guarantee that the ownership (and any changes thereof) takes place according to national laws and regulations, and that casinos typically have stringent systems in place to prevent fraud and safeguard against all criminal activity. Still, LEAs overall consider casinos the most exploited modus operandi to launder money through gambling activities despite the fact that casino activities have been covered by earlier EU AML legislation.

Conclusions:

Casinos are considered to be exposed to infiltration threats, although for State or public companies' owned casinos, this level of risk is lower. Nevertheless, LEAs still consider casinos the most exploited modus operandi to launder money through gambling activities. Hence, the risk of casinos being exploited to launder money appears high, and the level of ML threat related to casinos is thus considered as very significant. (level 4)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to casinos has not been considered as relevant. In that context, the TF vulnerability is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of ML vulnerability shows that the market is very different from one Member State to another.

(a) risk exposure:
Although the sector has developed alternative means of payment, in practice the use of cash is important and this sector may, in certain circumstances, be exposed to high risk customers (politically exposed persons or coming from high risk third countries). In addition, casinos are characterised by a high volume of financial transactions due to the high number of gambling activities it entails.

(b) risk awareness:
The inclusion of casinos in the list of obliged entities covered by 3rd AMLD has helped the sector in raising the level of its risk awareness. The legal framework already in place for casinos has for example created incentives for training of the staff and to improve controls. Casino staff is regularly informed and trained to identify patterns and behaviours considered to represent ML risks. These trainings include for instance measures and instructions on

handling of cash. Many land based casinos have developed inspections and controls systems by external and independent testing institutes which reduce the vulnerability to money laundering and criminal activities. Finally, the vast majority of land-based casinos have a CCTV system in place that oversees the areas of the casinos where transactions are being performed. Some CDDs are automatically performed as part of the identification process: all visitors before entering the casino, identification of visitors before purchase of chips/tickets and identification after a certain monetary threshold which is in most cases the EUR 2000 provided by 3rd AMLD but could be lower. Some casinos may decide not to identify the customer above a certain threshold when the individual has been identified through other means (i.e. at the entry into the casino or when purchasing chips). ECDD may apply for pre-defined high risk criteria, such as specific sums of money, transactions or structuring of operations.

According to some competent authorities and FIUs, some weaknesses still remain as regards the scope of the customer due diligence measures (which do not seem being well understood by the sector) and implementation thereof is not considered as satisfactory by the supervisors in all cases: e.g. checks on the ID card but record keeping requirements not fulfilled or of bad quality; customer due diligence when the customer enters the casino but not when one purchases chips. However, although the level of STRs is uneven depending on the Member State concerned, a low level of STRs is considered most of the times justified by the fact that the sector is strongly regulated and in general well controlled. The requirement to get senior approval for any high risk transactions is considered as limiting the risk of infiltration. Regarding STRs, stakeholders have stressed the lack of feedback from FIUs, and that the quality of the reporting would improve if FIUs would provide guidance and feedback, preferably within a set period of time.

(c) legal framework and controls

The inclusion of casinos in the list of obliged entities covered by 3rd AMLD has undoubtedly played a role in the quality of the controls in place. It appears that, overall, casinos manage to address the need to put in place several layers of controls, knowing that most of the time several gaming activities may be played in a casino.

From competent authorities' point of view, the most important vulnerability for casinos being the infiltration is rather well mitigated through fit and proper checks. Owners (shareholders), high ranking employees and key staff are systematically vetted by casino operators which grant rather efficient safeguards against risks of infiltration. Despite an overall good picture, there are still some weaknesses identified by LEAs which consider that the current legal framework is not correctly applied. The number of ML cases investigated by LEAs tends to demonstrate that there is still room for improvement.

Conclusions:

Although the risk exposure remains quite high (significant level of financial transactions; cash based), the inclusion of casinos in the AML framework for more than 10 years has raised the level of awareness to the ML risk vulnerability. Controls are more efficient and the staff is better trained. However, some weaknesses remain as regards the implementation of AML/CFT requirements, in particular, as far as CDD requirements are concerned. The extent of the reporting remains rather uneven from one Member State to another which may be justified by good level of controls. In that context, the level of ML vulnerability related to casinos is considered as moderately significant (level 2)

Mitigating measures

1) For competent authorities

- Member States should improve cooperation between relevant authorities (FIUs, LEAs, police, sectorial regulatory bodies such as gambling regulators) to better understand the risks factors inherent to casinos and to be able to provide efficient guidance.

- Member States should ensure a regular cooperation between relevant authorities and casinos. This better cooperation will focus on:

- strengthening the detection of suspicious transactions and to increase the number and the quality of the STRs;
- organising training sessions of the staff and compliance officers, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- provision by supervisory authorities of clearer guidance on AML/CFT risks, on CDD and on STR requirements and how to identify the most relevant indicators to detect money laundering risks.
- ensuring that FIUs provide feedback to casinos about the quality of the STR, ways to improve the reporting and about the use made of the information provided in, preferably within a set period of time;
- developing standardised STR/SAR template(s) at EU level taking into account specificities of gambling sector
- recommending the non-issuing of winning tickets certificates in casinos.

- Member States should require a reporting from competent authorities on the effectiveness of the AML/CTF regime applied by casinos as regards: the effectiveness of the controls undertaken through CCTV; the effectiveness of the threshold based CDD.

2) For the sector

- Member States should ensure that casinos organise training sessions of the staff and compliance officers on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly.
- Member States should ensure that casinos promote player's cards or use of electronic identification schemes, to facilitate the identification of the customer and to limit the use of cash and real-time monitoring systems to identify suspicious transactions.
- Member States should ensure that casinos designate an AML officer at the premises when it is not already the case
  Member States should ensure that betting operators promote systematic risk-based CDD of the winners, and promoting a lower threshold of winnings subject to CDD (currently at EUR 2000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission

The Commission should provide guidance on Article 11(d) concerning the implementation of CDD in case of "several operations which appear to be linked".

Gaming machines (outside casinos)

Product

Gaming machines (land-based/offline and outside casinos)

Sector

Gambling sector

General description of the sector and related product/activity concerned

Gaming machines (offline) based on a random number generator are normally divided into several subcategories, which depend on maximum stake, maximum winnings or the type of premises the gaming machine can be placed in. A further distinction is between traditional slot machines ("fruit machines") and Video Lottery Terminals which are connected to a central terminal and offer a wider range of forms of gaming.

The market for gaming machines outside casinos in the EU varies from one Member State to another (or region as authorizations may be granted and supervision assured at this level). In certain Member States gaming machines are prohibited outside casinos – others only permit machines with low stakes and low winnings.

In certain Member States, gaming machines can be found in a wide range of premises such as betting shops, arcades, bars and cafes. These terminals accept cash and provide a receipt providing evidence for the source of money. Where gaming machines are permitted, they may be subject to strict regulation as regards a fixed stake and limitations as regards gaming options – or the player may be able to interact more freely (e.g. fixed odds betting terminals (FOBTs), in the form of electronic roulette, where the player can select a number of options and vary the stakes).

Description of the risk scenario

A perpetrator deposits illicit funds (cash) into gaming machines or uses it to purchase tokens for the machines. Certain gaming machines also allow only a small part of the (deposited) amount to be staked, then requests the pay out of the remaining funds into a bank account or in cash with a receipt (thereby providing opportunities for legitimizing a larger sum than actually gambled).

A perpetrator uses electronic roulette to launder money placing even bets on both red and black, as well as a smaller stake on 0; the vast majority of the stake will never be lost as this is a 50/50 stake and there will be receipts confirming the winnings. Moreover, ticket In Ticket Out (*TITO*) vouchers from machines in casinos, arcades or betting shops can be used for money laundering and cashed in at a later date or by third parties.

A perpetrator can do all this repeatedly and/or in multiple venues to minimize suspicions or bypass limits on stakes or playtime.

Threat

Terrorist financing

The assessment of the TF threat related to gaming machines has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML threat related to gaming machines shows that as for all other gambling activities, one of the ML threat related to gaming machines is **the risk of infiltration or ownership by organised crime groups**. However, from LEAs investigations, it seems that cases are quite rare or not reported. It may not be considered as a very viable or attractive financial option as the chance of winning large amounts is relatively low (outcome based on chance, often with low stakes and low winnings), although in the case of some machines there are ways to increase chances of winning or even avoid playing; and merely pay in and pay out funds.

Conclusions: Gaming machines do not appear to be an attractive option for ML purposes due to the inherent chance element, amounts of stakes and winnings combined with the time and efforts required to launder any significant amounts of money. However, certain types of gaming machines allow deposits of higher stakes and/or winnings; or to stake only a small part of the amount requesting a pay-out of the remaining funds (into a bank account or in cash with a receipt). In this context, although the level of ML threat may vary in between different types of gaming machines (low/high stakes and/or winnings) it is generally considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to gaming machines has not been considered as relevant. In that context, the TF vulnerability is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML vulnerability related to gaming machines shows that:

(a) risk exposure:

Gaming machines (land-based) rely mostly on cash. Transaction amounts vary, tend to be rather low but certain machines offer the possibility of also staking higher amounts.

(b) risk awareness:

For gaming machines outside casinos, the risk awareness is different from one Member State to another and it seems that independent gaming machines operators are less aware about their AML/CFT obligations, due to the fact that they are less organised than when occurring in land-based casinos.

Competent authorities have, in addition, noticed the emerging risk linked to video lotteries (VLTs) which trigger a growing number of STRs (because in general, the winnings are re-injected in the dark economy).

(c) legal framework and controls in place:

Gaming machines are not covered by the current EU AML framework (3AMLD). However, based on minimum harmonisation principles of it, some Member States have already extended their national AML/CFT regimes to gaming machines. This has created discrepancies from one Member State to another in term of regulation, supervision of the sector and enforcement of AML/CFT rules.

Some Member States have decided to regulate this sector when it operates separately from casinos. According to competent authorities and FIUs, the level of controls is insufficient and the level of sanctions not dissuasive enough (e.g. a bookmaker in a Member State X received a fine of more than EUR100 000 for failing to prevent a drug dealer from laundering over EUR 1 million in its outlets). However, gaming machines operators are currently developing some mitigating measures, by prohibiting pay-out of winning in cash when exceeding certain amounts.

Conclusions:

For gaming machines outside casinos, it appears that controls in place are not efficient and that the level of STR is quite low, although mitigating measures in order to limit the pay-out in cash tend to limit the risk of ML. Even if the amounts of stakes and winnings are often relatively low, it allows for speedy and anonymous (as well as repeated) transactions, often cash based, with possibilities to carry out the transactions in multiple venues to minimize suspicions or bypass limits on stakes or playtime. In that context, the level of ML vulnerability for gaming machines is considered as moderately significant (level 2).

Mitigating measures

1) For competent authorities

- Member States should improve cooperation between relevant authorities (FIUs, LEAs, police, sectorial regulatory bodies such as gambling regulators) to better understand the risks factors inherent to gaming machines and to be able to provide efficient guidance.
- Member States should ensure a regular cooperation between relevant authorities and gaming machine operators. This better cooperation will focus on:

- strengthening the detection of suspicious transactions and to increase the number and the quality of the STRs;
- organising training sessions of the staff, compliance officers and retailers, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- provision by supervisory authorities of clearer guidance on AML/CFT risks, on CDD and on STR requirements and how to identify the most relevant indicators to detect money laundering risks;
- provision by supervisory authorities of clearer guidance on emerging risk linked to video lotteries (VLTs);
- ensuring that FIUs provide feedback to gaming machine operators about the quality of the STR, ways to improve the reporting and about the use made of the information provided in, preferably within a set period of time;
- developing standardised STR/SAR template(s) at EU level taking into account specificities of gambling sector

2) For the sector

- Member States should ensure that gaming machines operators organise training sessions of the staff, compliance officers and retailers are organised on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- Member States should ensure that gaming machines operators promote player's cards, or use of electronic identification schemes, to facilitate the identification of the customer and to limit the use of cash, and real-time monitoring systems to identify suspicious transactions at point of sales;
- Member States should ensure that gaming machines operators designate an AML officer at the premises when it is not already the case
  Member States should ensure that betting operators promote systematic risk-based CDD of the winners, and promoting a lower threshold of winnings subject to CDD (currently at EUR 2000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission

The Commission should provide guidance on Article 11(d) concerning the implementation of CDD in case of "several operations which appear to be linked".

Lotteries

Product
Lotteries
Sector
Gambling sector
General description of the sector and related product/activity concerned
Lotteries cover a wide range of numeric games where a winner is selected by chance. Lotteries range from National Lotteries that has been granted an exclusive license to operate lottery games on its territory (state-owned and private operators, both profit and non-profit, who operate on behalf of the state), to small charity lotteries that both generate revenues for the public benefit or non-profit organizations (e.g. charities, civil society, sport, culture, heritage, social welfare). The definition of lotteries – or the requirements to obtain a license – varies from one Member State to another. Tickets in a national lottery are normally sold through agents sold for cash or through card transactions or directly to the player online. Small amounts are played in most of the cases. Winners can be selected instantly (e.g. so called 'scratch- cards') or on the basis of weekly draws (often highly promoted and televised). Winnings are either paid out by the agents after presenting a winning ticket (small amounts) or directly transferred to the player's bank account (large amounts and jackpots). The returns on stakes are normally lower than for other gambling products as the purpose is to raise funds for the public good (40- 50% of the funds collected are normally returned as prizes – but there are examples where the rate of return is higher. The chance of winnings jackpot is very low (e.g. Euro Millions rank 1 jackpot one chance up to 139.838.160)
Description of the risk scenario
The relatively low return to players makes direct purchase of lottery tickets a costly and unattractive form of money laundering. Direct purchase of lottery tickets to win a prize is therefore not considered a likely risk scenario. On the contrary, the modus operandi of purchasing a winning ticket - a perpetrator purchases a lottery ticket from the winner (possibly through collusion with the sales agent) and cashes the prize with a receipt is more viable scenario reported by LEAs.
Threat
Terrorist financing The assessment of the TF threat related to lotteries has not been considered as relevant. In that context, the TF threat is not part of the assessment. **Conclusions: not relevant**

Money laundering

The assessment of the ML threat related to lotteries shows that

- as it is the case for all other gambling activities, it is not excluded that one of the ML threat related to lotteries would be **the risk of infiltration or ownership by organised crime groups.** In case of State-owned lotteries, the risk seems minimal, but increases at the level of retailers.

- for other kinds of threats, according to LEAs, criminals have only vague intentions to use this scenario to launder proceeds of crime. Few cases have been identified by LEAs where for example winning tickets have been found together with cash or drugs in seizures. But if and when used, this scenario may allow collecting large sums of cash (e.g. investigation has revealed the collect of 1,2MEUR via winning tickets). It requires nevertheless some planning capabilities and technical expertise which in general requires the complicity of the lottery house and the reliance on front-men. This could limit criminals' intent to use this risk scenario. It has also been pointed out that lotteries offer less opportunities in terms of money laundering due to lower frequency of play (draw games), low average stakes and winnings (instant tickets and numerical games and low pay-out ratio). In general, lotteries as such would not be specifically attractive to launder proceeds of crime referring to the relatively low return rate (most of the time only 50% of the ticket sales are used for prizes).

Conclusions: Cases where lotteries are used to launder proceed of crimes have been reported. However, it requires planning and expertise that may limit the intent and capability of organised crime organisations to use it. The specific modus operandi with purchasing of winning tickets appears though to be a more viable and reported scenario. In this context, ML threat related to lotteries is considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to lotteries has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML vulnerability related to lotteries shows that

(a) risk exposure:
In assessing the level of risk exposure it is also taken into consideration that in many Member States, lotteries are under State monopoly and payments of higher winnings are subject to rigorous controls and most lottery operators limit the prizes that can be paid out by retailers. Major prices are cashed at lottery headquarters and/or banks (under contractual agreement between the operator and the chosen bank) following strict verification procedures on both the validity of the prize claim and the winner's identity. However, winnings under a certain threshold (i.e. small amounts), varying from Member States, are paid directly by sales agents/authorised distributors. Furthermore the anonymity of the player is in many Member States guaranteed which makes it more difficult for criminals to identify the holder of the winning ticket to be purchased for criminal purposes, unless the active help of accomplices.

(b) risk awareness:
While the misuse via the purchase of winning tickets is considered as an important concern for FIUs and LEAs (including quite often collusion with sales agents), the general level of awareness is rather difficult to assess. Although identification of players falls under direct control of retailers, who operate under the authorisation of the operator, with specific sanctions on them, it has been mentioned that the lottery operators are active in the control on the authorised retailers and coordinate retailer training programs in AML awareness/detection.

(c) legal framework and controls

Lotteries are not covered by the current EU AML framework (3AMLD). However, based on minimum harmonisation principles of it, some Member States have already extended their national AML/CFT regimes to lotteries. This has created discrepancies from one Member State to another in term of regulation, supervision of the sector and enforcement of AML/CFT rules.

However, at national level, supervision by competent authorities works well and is undertaken by public authorities in general. It has for example been pointed out that most gambling authorities have already introduced recommended procedures and controls to deter criminals from using the lottery facilities for money laundering. Additionally, lottery operators have established internal controls and heightened vigilance in these matters. For example, the control on the identification and verification of the jackpot winners' identity where the prize exceeds a predetermined threshold is already in place in most Member States.

Conclusions: Based on the vulnerability assessment, it appears that lotteries as such are not a viable risk scenario but that the risks are more related to (purchasing of) winning tickets. Although lottery operators are currently not considered as obliged entities in the whole EU, national frameworks in place have introduced control and identification measures, in particular relating to high winnings. Still, the (purchasing of) winning tickets risk scenario remains an important point of concern. On this basis, the level of ML vulnerability related to lotteries is considered as moderately significant (level 2).

Mitigating measure

1) For competent authorities

- Member States should improve cooperation between relevant authorities (FIUs, LEAs, police, sectorial regulatory bodies such as gambling regulators) to better understand the risks factors inherent to lottery activities and to be able to provide efficient guidance.
- Member States should ensure a regular cooperation between relevant authorities and lotteries operators. This better cooperation will focus on:

- strengthening the implementation of CDD requirements, the detection of suspicious transactions especially in the context of winning tickets and to increase the number and the quality of the STRs;
- organising training sessions of the staff, compliance officers and retailers, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- provision by supervisory authorities of clearer guidance on AML/CFT risks, on CDD and on STR requirements and how to identify the most relevant indicators to detect money

laundering risks;
- ensuring that FIUs provide feedback to lottery operators about the quality of the STR, ways to improve the reporting and about the use made of the information provided in, preferably within a set period of time;
- developing standardised STR/SAR template(s) at EU level taking into account specificities of gambling sector

2) For the sector

- Member States should ensure that lottery operators organise training sessions of the staff, compliance officers and retailers on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly. Training would also include elements related to appropriate red flags on repetitive winnings
- Member States should ensure that lotteries promote systematic identification of winners; player's cards, or use of electronic identification schemes, to facilitate the identification of the customer, and the use of account-based fund transfers for payments of large amounts
- Member States should encourage lotteries to designate an AML officer at the premises when it is not already the case
- Member States should ensure that betting operators promote systematic risk-based CDD of the winners, and promoting a lower threshold of winnings subject to CDD (currently at EUR 2000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission

The Commission should provide guidance on Article 11(d) concerning the implementation of CDD in case of "several operations which appear to be linked".

Poker

Product

Poker (land-based/offline)

Sector

Gambling sector

General description of the sector and related product/activity concerned

General description of the sector (size) and statistics and related product/activity concerned

Poker is a card game that involves betting procedures and where the winner of each hand (round) is determined according to the combinations of players' cards and the bets, at least some of which remain hidden until the end of the hand.

Poker is organized by private operators or state owned gambling service providers in licensed premises (such as casinos), private clubs or online (depending on national legislation). It is either organized as a tournament, where a poker player enters by paying a fixed buy-in and at the start of poker tournament and given a certain amount of poker chips (the winner of the tournament is usually the person who wins every poker chip in the tournament) or as a table game where the player can buy more poker chips as the game continues. Unlike many other gambling products, participants play against each other and not against the organizer of the activity. The organizer will receive a fixed amount of the turnover (a rake) or winnings.

Poker may also be played in private clubs (*cercles de jeux*) which exist in some jurisdictions but are banned in others and tournaments can be organised outside casinos.

Description of the risk scenario

A perpetrator purchases chips at the casino (or at the relevant licenced premises) at a dedicated point of sale (for cash or anonymous pre-paid cards) and these chips may be transferred to another player through deliberate losses (fold on a winning hand to ensure that the accomplice receive the chips). Chips are converted into cash or transferred in another way to the customer.

A perpetrator (organised crime organisations) may also seek to infiltrate the organisational structure of the licenced premises where poker games or tournaments are organised (e.g. casinos or private clubs) or directly or indirectly apply for a licence to organise a poker tournament, which may be open or on invitation only.

Threat

Terrorist financing

The assessment of the TF threat related to poker has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML threat related to poker shows that

- as for all other gambling activities, one of the ML threat related to poker is **the risk of**

infiltration or ownership by organised crime groups.

- the modus operandi is perceived as rather attractive although it requires moderate levels of planning (complicity) or technical expertise (gaming strategy itself) using illicit tournaments or in view of the possibility to make deliberate losses/winnings.

Conclusions: In addition to the risk of infiltration of a company that holds a licence to organise poker games or tournaments in physical premises (which is a horizontal threat that also is valid for other gambling service providers) there is in some Member States a possibility to organise individual tournaments. Criminal organisations could also legally organise poker games/tournaments. The peer-to-peer gambling nature of poker (the possibility for deliberate losses/winnings to another player) makes poker attractive to money laundering, although it requires some expertise and planning. In that context, the level of ML threat related to poker is considered as significant (level 3).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to poker has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML vulnerability related to poker presents

(a) risk exposure:
Most of the time, poker games are organised in the premises of licensed casinos. "Private" poker club are prohibited and considered as illicit activities in most Member States. However, even when played within casinos, poker is vulnerable to money laundering as it allows the use of cash based transactions and involves peer-to-peer element (simplifying deliberate losses/winnings to another player). Poker game allows to process significant volumes of speedy and anonymous transactions from one player to another (and chips are frequently bought for cash).

(b) risk awareness:
The level of awareness is difficult to assess at this stage, as most of the time poker games are organised within casinos. A dedicated analysis is challenging to conduct.

(c) legal framework and controls:
Poker activities (outside casinos) are not covered by the current EU AML framework (3AMLD). However, based on minimum harmonisation principles of it, some Member States have already extended their national AML/CFT regimes to poker. This has created discrepancies from one Member State to another in term of regulation, supervision of the sector and enforcement of AML/CFT rules.
Players play against other players (peer-to-peer) and there is no records on 'who-lost-to-whom'. An emergence of unauthorised poker private clubs, which are well organised and compete with the legal sector, has also been noted. FIUs consider that they have low capacity to detect the suspicious transactions, especially because the sector itself is not well aware about the risks and/or not sufficiently regulated/supervised at national level.

Conclusions:

Considering the peer-to-peer element, apparent lack of record keeping and proper supervision and that the sector itself is not well aware of its risks and/or well equipped against ML abuses. The level of ML vulnerabilities related to poker is considered as significant (level 3).

Mitigating measures

1) For competent authorities

- Member States should improve cooperation between relevant authorities (FIUs, LEAs, police, sectorial regulatory bodies such as gambling regulators) to better understand the risks factors inherent to poker and to be able to provide efficient guidance.
- Member States should ensure a regular cooperation between relevant authorities and poker operators. This better cooperation will focus on:

- strengthening the implementation of CDD requirements, the detection of suspicious transactions and to increase the number and the quality of the STRs;
- organising training sessions of the staff and compliance officers, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly;
- provision by supervisory authorities of clearer guidance on AML/CFT risks, on CDD and on STR requirements and how to identify the most relevant indicators to detect money laundering risks;
- ensuring that FIUs provide feedback to poker operators about the quality of the STR, ways to improve the reporting and about the use made of the information provided in, preferably within a set period of time
- developing standardised STR/SAR template(s) at EU level taking into account specificities of gambling sector

2) For the sector

- Member States should ensure that poker operators organise training sessions of the staff and compliance officers on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly.
- Member States should ensure that poker operators promote player's cards, or use of electronic identification schemes, to facilitate the identification of the customer
- Member States should ensure that poker operators designate an AML officer at the premises when it not already the case
- Member States should ensure that betting operators promote systematic risk-based CDD of the winners, and promoting a lower threshold of winnings subject to CDD (currently at EUR 2000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission

The Commission should provide guidance on Article 11(d) concerning the implementation of CDD in case of "several operations which appear to be linked".

Online gambling

Product

Online gambling

Sector

Gambling sector

General description of the sector and related product/activity concerned

For this purpose, online gambling means any service which involves wagering a stake with monetary value in games of chance, including those with an element skill, such as lotteries, casino games, poker games and betting transactions that are provided by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.

All gambling products are available online - both games where the customer wager a stake against the gambling service provider at fixed odds (e.g. lotteries, sports betting, roulette etc.) and gambling activities where customers can play against each other and where the service provider takes a small commission, a percentage of net winnings for each customer on each event, for facilitating the activity (e.g. poker and betting exchanges where customers can both place and accept bets).

However, a further division into different online gambling products has not been considered necessary for this purpose, at this stage, as the relevant risks, threats and vulnerabilities appear to be primarily linked to the nature of online transactions generally rather than to specific forms of online gambling

Description of the risk scenario

Online gambling could involve any product in the gambling sector or a combination of these. In addition to some of the risks identified for each sector offline, there may be additional risks associated with the lack of face-to-face contact enabled by the Internet. At the same time, electronic gambling offers an important mitigating feature in the possibility of tracking all transactions.

A perpetrator uses gambling sites to deposit illicit funds and to request the pay out of winnings or unplayed balance.

Legitimate online gambling accounts are credited with dirty funds (cashing in) followed by gambling on only small amount of funds, transferring the remaining funds to a different player (or to a different online gambling operator). The remaining funds are cashed out as if they were legitimate gambling earnings.

Crime organisations may use several "smurfs" betting directly against each other using dirty funds. One of the "smurfs" will receive all the funds as an apparent winner, who will then cash out the funds as it they were legitimate gambling earnings.

Crime organisations may purchase online casino accounts containing funds already uploaded by non-criminal players at a higher price than the real one.

Crime organisations may also invent and bet on fictitious (non-existing) matches or events to ensure winnings.

Threat

Terrorist financing

The assessment of the TF threat related to online gambling has not been considered as relevant for the purpose of this first SNRA. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML threat related to online gambling shows that:

- as for all other gambling activities, one of the ML threat related to online gambling is **the risk of infiltration or ownership by organised crime groups.** LEAs have several examples where such cases occur.

- in addition, organised crime groups may easily have access to such modus operandi which is cheap and practical to set up. It represents an attractive tool to launder proceeds of crime. It could allow easy conversion from criminal money to legitimate gambling earnings. It involves huge volume of transactions and financial flows.

- risks associated with the lack of face-to-face contact although the anonymity can be minimised by proper controls and verification measures, as well as traceability and tracking of electronic transactions depending on the level of supervision by relevant authorities.

Conclusions: LEAs consider online gambling to be a potentially attractive tool to launder money which requires a moderate level of expertise and represents a viable option. Also, online gambling appears to offer a low cost opportunity to launder money. In that context, the level of ML threat related to online gambling is considered as significant (level 3)

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to online gambling has not been considered as relevant. In that context, the TF threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the ML vulnerability related to online gambling shows that

(a) risk exposure:

The risk exposure of online gambling is characterised by two components:

- the non-face-to-face element of the business relationships (considered as factor of high risk both in the EU framework and in FATF requirements) and
- the possibility to use less traceable means of payments on the online platform (i.e. anonymous/prepaid e-money, or even virtual currencies where they are allowed).

In effect, online gambling allows worldwide operations on a 24/7 basis. It involves a huge

volume of transactions and financial flows. It does not involve physical products and makes more difficult the detection of the suspicion. Although online gambling is not cash based, it is closely connected to the use of other products such as e-money or virtual currencies which present their own set of ML risks. The non-face-to-face nature of online gambling increases the degree of anonymity. It is also important to mention that LEAs (including EUROPOL) have noticed an increased trend in the creation of unlicensed gambling sites which are not subject to CDD, record-keeping and reporting requirements. They are not audited by a supervisory authority. This may create important impacts for the EU internal market when these unlicensed gambling sites are incorporated outside the EU and engage easily with EU customers over the Internet.

At the same time, these vulnerabilities should take account the fact that online gambling may also rely on bank or payment accounts where the customer is already identified and submitted to basic CDD.

(b) risk awareness:

The level of awareness of the online gambling sector depends on the existence of AML/CFT legislation or not. When covered by the AML/CFT requirements, the level of STR is quite good and controls in place as well (automatic checks in place). Some national legislation provides that for e-wallets, funds are sent back to the player on the same account. In addition, when prepaid cards are used, in general, only small amounts are at stake.

Attention has been drawn to the fact that large parts of the sector have put in place AML trainings for every employee within the company. Employees are also given training material on the practical issues such as the characteristics of the suspicions, how to escalate them to the compliance officer and further information about how to tackle the issues on an operational level. Representatives of online gambling operators note that FIUs do not offer feedback on STRs submitted which causes difficulties for operators on individual cases (where it is unclear whether funds should be paid out to a player who may in turn take action against the operators) and prevents improvements to AML practices in general. This may even discourage future reporting. There is also a perception of conflict with data protection rules, which may decrease the level of reporting. Nevertheless, they also flagged that most of the times competent authorities provide risk assessment in order to help obliged entities in improving their understanding of the risks. While the overall risk based approach remains valid, some operators regret the lack of clear guidance on when and how an operator shall apply its AML/CFT obligations. Thus, in many cases, there is a discrepancy between competent authorities' understanding of the risks and the reality check proposed by online gambling operators.

(c) legal framework and controls

Online gambling (except casinos) is not covered by the current EU AML framework (3AMLD). However, based on minimum harmonisation principles of it, some Member States have already extended their national AML/CFT regimes to online gambling and/or through requirements in licensing agreements. This has created discrepancies from one Member State to another in term of regulation, supervision of the sector and enforcement of AML/CFT rules

Some operators licensed in one or more Member States offer gambling services also in other Member States, without authorisation. In addition, gambling operators based outside EU jurisdictions operate unauthorised in the EU (that is without having been licenced in any EU Member State and thus outside any control within the EU).

There are some situations where the online gambling platform is situated in one Member State and the e-money issuer providing the funds in another Member State. Sometimes, platforms

are licensed in one territory but operate in another one through an intermediary (which may or may not be considered as an establishment). In such situations, some authorities do not always find it clear where the reporting shall occur (host/home FIU) and where the supervisory actions shall take place (host/home supervisors). Hence, competent authorities and obliged entities consider that the current legal framework is not always clear enough to understand which authority is competent to apply AML/CFT requirements.

There is no duty of mutual-recognition principle of authorisations issued by the EEA Member States. Also given the large margin of discretion for Member States to regulate gambling activities, including online gambling, and that supervision and enforcement are matters for the national authorities, the consequence is that regulations and controls in place vary.

Conclusions:

Despite several risk-based measures already being implemented by many online operators (for example AML trainings for employees, CDD and KYC processes), the risk exposure to ML risks of online gambling is still rather high due to the fact that it encompasses important factors such as non-face-to face element, complex and huge volumes of transactions and financial flows. Although not cash based, it is closely connected to the use of e-money, digital and virtual currencies which, for example, also increases the degree of anonymity for customers. As recognized, in many Member States, online gambling operators have developed a good level of self-regulation and risk assessment, although the cooperation with competent authorities and FIUs could be improved. Operators consider that they do not benefit from clear guidance on how to address properly the risks considering in particular the lack of feedback from FIUs on STRs. In that context, the level of ML vulnerability related to online gambling is considered as significant (level 3).

Mitigating measures

1) For competent authorities/regulators

- Member States should improve cooperation between relevant authorities (FIUs, LEAs, police, sectorial regulatory bodies such as gambling regulators) to better understand the risks factors inherent to online gambling and to be able to provide efficient guidance.
- Member States should ensure a regular cooperation between relevant authorities and online gambling operators. This better cooperation will focus on:
  - strengthening the implementation of CDD requirements, the detection of suspicious transactions and to increase the number and the quality of the STRs, in particular in situation of cross-border use of the online gambling platform
  - organising training sessions of the staff and compliance officers, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly
  - provision by supervisory authorities of clearer guidance on AML/CFT risks, on CDD and on STR requirements and how to identify the most relevant indicators to detect money laundering risks.
  - raising awareness of online gambling operators on emerging risks factors that may impact the vulnerability of the sector such as the use of anonymous e-money or virtual currency or the emergence of unauthorised online gambling operators
  - raising awareness and increasing regulators and competent authorities' capacity/expertise to assess risks in the online environment/ cyber security and to detect and prevent ML; in this regard, pooling resource with other Member States

(for example by organising joint training) could be considered.

- Member States are encouraged to require from the supervisory competent authorities, where appropriate, to publish a report on the safeguards put in place by online gambling operators to limit the risks posed by non-face-to-face business relationships (online identification and checks, monitoring of the transaction);
- Member States should ensure that FIUs provide feedback to online gambling operators about the quality of the STR, ways to improve the reporting and about the use made of the information provided in, preferably within a set period of time;
- Member States should develop standardised STR/SAR template(s) at EU level taking into account specificities of gambling sector
- Member States should ensure that specific safeguards for non-face-to-face business relationship are used such as electronic identification (E-IDAS identification, electronic signature);
- Member States should provide guidance on the interplay between CDD requirements and data protection rules and on reporting.

2) For the sector

- Member States should ensure that online gambling operators organise training sessions of the staff and compliance officers on a regular basis, with particular focus on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model to be reviewed regularly.
- Member States should ensure that betting operators promote systematic risk-based CDD of the winners, and promoting a lower threshold of winnings subject to CDD (currently at EUR 2000 as provided by Article 11 d) of Directive (EU) 2015/849).

- Member States should ensure that online gambling operators designate an AML officer at the premises when it is not already the case.

3) For the Commission

The Commission should provide guidance on Article 11(d) concerning the implementation of CDD in case of "several operations which appear to be linked".

Non-for-profit organisations

Collect and transfers of funds through a Non-Profit Organisation (NPO)

Product
Collect and transfers of funds through a Non-Profit Organization
Sector
Non-Profit Organizations sector
General description of the sector and related product/activity concerned
Following FATF guidance, NPOs include the following sectors: 1/ “service activities", meaning programmes focused on providing housing, social services, education, or health care. They may cover for example NPOs engaged in humanitarian aid or development assistance, as well as NPOs carrying out other activities. As far as humanitarian NPOs are concerned, the objective of humanitarian aid is to save and preserve lives of people affected by natural or man-made disasters, in full respect of International Humanitarian Law and of the humanitarian principles of humanitarian action, neutrality, impartiality, humanity and independence. Humanitarian NPOs may be active within distinct geographical (within and outside of Europe) and operational contexts. Nonetheless, a large part of humanitarian aid is carried out in or is connected to the consequences of armed conflicts and other situations of violence. Also, humanitarian organisations may operate in some regions and countries where persons and entities designated as "terrorist" are present and likely to pursue their activities. While the humanitarian aid sector accommodates a wide range of organisations of various degrees of operational and organisational capacity, there is an important segment of NPOs receiving institutional humanitarian aid funding, among others by the EU and and Member States in charge of the management of EU funds, and are subject to a strict contractual framework with a high degree of safeguards. EU humanitarian aid funding is managed by the European Commission and is channelled through partners, including NPOs, which are selected based on specific legal, financial and operational criteria, and are signatories of a Framework Partnership Agreement (FPA). 2/ "expressive activities”, meaning programmes focused on sports and recreation, arts and culture, interest representation or advocacy such as political parties, think tanks and advocacy groups. They are in general NPOs engaged in philanthropy activities.
Description of the risk scenario
• Establishment of NPOs to "fund raise" whereby criminals funds are gradually sent to the NPOs: - complicit NPOs may intentionally support a terrorist group or a criminal organisation - legitimate NPOs may be exploited by "outsiders" - legitimate NPOs may be exploited by "insiders". • Criminals may abuse NPOs to fund localised terrorist activities, or may seek to use NPOs to facilitate cross-border financing by sending money to areas where the NPOs

are operating close to terrorist areas of activity

- complicit NPOs may intentionally support a terrorist group or a criminal organisation
- legitimate NPOs may be exploited by "outsiders"
- legitimate NPOs may be exploited by "insiders".

General comments (if relevant)

For this risk assessment, it is agreed that NPOs shall be understood as defined in FATF standards (Recommendation 8): expressive NPOs and service NPOs. This assessment will be about all categories of NPOs falling under the FATF definition, to avoid singling out one category of NPO. This risk scenario is intrinsically linked to transfers of funds – NPO.

As the assessment concerns money laundering and terrorist financing affecting the internal market and cross-border activities, this exercise is relevant both for the collection of funds within the internal market and for the collection and transfer of funds from within the EU to third countries.

Threat

Terrorist financing

The assessment of the TF threat related to collect and transfers of funds by NPOs shows that this modus operandi is not really frequently used by terrorist groups. Indeed, based on the number of NPOs registered, very few are misused. However, existing NPOs may be concerned by the risk of being infiltrated by terrorist groups which may represent a significant threat, in particular as far as foreign terrorist fighters are concerned. In general, collect and transfers of funds through NPOs does not require specific expertise. However, terrorist groups may need more particular knowledge and skills to pass the registration test to enter the NPO. Once infiltrated, the NPO is may be attractive to finance terrorist activities.

As far as humanitarian NPOs are concerned, while there are some inherent risks in humanitarian work taking place at times in high risks areas with presence of non-state armed groups or persons designated as terrorists, the concrete risks depend on various factors, such as the level of 'professionalization' of an NPO, each individual country situation, including the political dynamics of the conflict in question..

Conclusions: The NPO landscape is fairly broad. Considering that NPOs are quite easy to infiltrate (low level of controls – see vulnerability assessment), the access to funds collected or transferred by NPOs to finance terrorist activities is quite attractive and does not require specific technical expertise. At the same time, only few NPOs are concerned by this threat. In that context, the level of threat for TF is considered as significant (level 3). For NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, the level of threat is however considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to collect and transfers of funds through NPOs has been considered in conjunction with TF schemes related to collect and transfers of funds through NPOs in order to fund terrorist activities. In that context, the ML threat does not benefit from a separate assessment.

Conclusions: In that context, the level of threat for ML is considered as significant (level 3). For NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, the level of threat is however considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to collect and transfers of funds by NPOs shows that:

General remarks: the analysis of the NPO sector from a vulnerability perspective is quite complex.

- On the basis of the work undertaken by the FATF, the TF vulnerability has demonstrated that there was an interest to build on the FATF distinction between *expressive NPO* (NPOs predominantly involved in expressive activities, which include programmes focused on sports and recreation, arts and culture, interest representation, and advocacy) and "*service NPOs'* " (NPOs involved in diverse activities, including but not being limited to humanitarian services). Competent authorities and FIUs agree to consider that the two categories present differences in their risk exposure and risk awareness.
  Expressive NPOs present some vulnerability because they can be infiltrated by terrorist organisations that can hide the beneficial ownership making the traceability of the collect of funds less easy.

  Service NPOs are more directly vulnerable due to the intrinsic nature of their activity (NPOs on the field): they may be located in conflicts/war areas; in high risk third countries; have high risk customers.
- However, this distinction does not prevent from drawing common characteristics of the NPOs sector vulnerabilities. Some Member States even tend to consider that this distinction is not relevant and that, whatever the category of NPOs concerned, the sector is characterised by a variety of structures and activities which can have an impact on the level of risk awareness and risk exposure.

(a) risk exposure:

As mentioned above, there is an inherent risk for NPOs working in high risk areas and exposed to high risk customers. A part of the funding is channelled through cash which make the traceability of source of funds but also of the transfers (when sent abroad) difficult from LEAs and FIUs points of views.

As far as humanitarian NPOs are concerned, while there are some inherent risks in humanitarian work taking place at times in high risks areas with presence of non-state armed groups or persons designated as terrorists, the concrete risks depend on the level of 'professionalization' of an NPO, each individual country situation, including the political dynamics of the conflict in question. **(b) risk awareness:**

NPO sector has no centralised organisational framework and the rules applicable to it are not harmonised at EU level and vary from one Member State to another. This lack of centralized organisation limits competent authorities' ability to provide some guidance or assistance. The risk awareness is increasing in the NPO sector. NPOs voluntarily undertake their own risk assessment which takes consideration of the geographic location, the type of activity, the history of the engagement in the area. They are starting developing controls and due diligence

measures on transfers and collects of funds (sanctions lists screening). The sector is also developing peer-learning exchanges on due diligence practices, transparency and accountability questions and risk management as well as awareness raising events on terrorist financing. NPOs actors (in particular from philanthropy) are becoming more and more aware of risks, in particular, where financial transactions are taking place outside of the financial system. There is also greater collaboration and outreach to the banking sector to facilitate safe and regulated channels for legitimate humanitarian causes, thereby increasing transparency and helping to safeguard NPOs from terrorist abuse, while at the same time allowing delivery of humanitarian aid to regions most in need. The sector is engaged in self-regulation's actions, with the issuance of codes of conduct developed both by the fundraising as the philanthropic sectors which often include governance, reporting, monitoring of the use of funds "know your donors" and "know your beneficiaries". Finally, NPOs that receive institutional humanitarian aid funding from the EU and Member States in charge of the management of EU funds are subject to a strict contractual framework, with a higher degree of safeguards. While acknowledging the vital importance of the NPO community, among others in providing humanitarian assistance around the world, and the need to safeguard the legitimate objectives of humanitarian aid, more awareness raising within the NPO sector of TF risks may be needed to enhance the risk awareness within the NPO sector

(c) legal framework and controls in place:

NPOs are not included in the AML/CFT framework at EU level. Their coverage by AML/CFT rules is left to Member States discretion. The existing AML/ CFT requirements are not necessarily considered as adequate to address the specific needs of the NPO sector and controls in place are not equal depending on the Member State concerned. The conditions of registration of NPOs are also not the same. Competent authorities tend to consider that controls in place are quite good concerning the collection of funds within the EU. However, some weaknesses appear when dealing with transfers of funds or expenditures outside the EU.

It is important to note that, beyond AML/CFT requirements, humanitarian NPOs are governed by the Humanitarian Principles that are humanity, impartiality, neutrality and independence. As far as specific categories of humanitarian NPOs are concerned, notably those that have been assessed by the European Commission, it is also important to note that beyond the strict eligibility and suitability criteria, checked through a detailed selection process prior to the signature of the FPA, there are also continued checks during the lifetime of the partnership and specific humanitarian actions, such as detailed reporting on actions, obligations on record keeping, as well as regular audits, both at HQ and in the field.

As far as the legal framework is concerned it is relevant to note that a balance needs to be found between the counter-terrorism agenda and the legitimate objectives of humanitarian NPOs. For example, the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA includes a humanitarian exemption for humanitarian activities by impartial humanitarian organisations.

Conclusions: the risk exposure of the NPOs is impacted by the intrinsic nature of their activities, various degree of risk awareness exist, mostly due to a fragmented NPO landscape. The applicable legal frameworks and national practices are diverse while it should be acknowledged the specific setup of the humanitarian sector described above. In that context, the level of TF vulnerability is considered as significant (level 3). For NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, the level of threat is however considered as moderately significant (level 2).

Money laundering

The assessment of the ML threat related to collect and transfers of funds through NPOs has been considered in conjunction with TF schemes related to collect and transfers of funds through NPOs in order to fund terrorist activities. In that context, the ML threat does not benefit from a separate assessment.

Conclusions: In that context, the level of vulnerability for ML is considered as significant (level 3). For NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, the level of vulnerability is however considered as moderately significant (level 2).

Mitigating measures

1) For the Commission:

- To provide Commission guidance and/or training to NPO in receipt of EU funding on the relevant EU legal framework, as well as on how to identify risks and meet due diligence requirements.
  To organise multi-stakeholders exchange involving all professional sectors, in particular the financial sector, involved in business with NPOs

2) For competent authorities

- Member States should ensure better NPO involvement into national risk assessments, into the development of informational and awareness programs designed to counteract the risk of being abused - support NPOs by providing awareness raising materials for NPOs (at member State as well as at EU level)
- Member States should also further analyse the risks faced by NPOs sector

Horizontal vulnerabilities

Vulnerabilities linked to financial supervision

Vulnerabilities linked to supervision, cooperation between financial supervisors and passporting (cross border activities by FI's under free provision of services and freedom of establishment)

This description relates to horizontal vulnerabilities which were mentioned for different sectors regulated by AMLD. The level of materiality of those vulnerabilities has been assessed in the respective product risk fiches. This paper covers only horizontal issues and possible mitigating measures of horizontal aspects.

Assessment of vulnerability

I. National and cross border supervision: cooperation

Competent authorities do not always cooperate effectively in relation to AML/CFT supervision of firms that operate on a cross-border basis.

Relevant AML/CFT supervisory information is not/not sufficiently/not timely shared amongst the competent AML/CFT supervisors at national and EU level. This may negatively impact the effectiveness of the AML/CFT supervision of FI's (including the corrective measures and sanctioning in case of non-compliance), both at national and EU level. The underlying reasons can be as follows:

1. Non-cooperation or refusal to cooperate between financial AML/CFT supervisors based on the argument that the counterpart has a different nature or status

- E.g. some competent authorities consider that national or supranational legal provisions prevent the sharing of information with other AML/CFT competent authorities that have a different legal status, for example, because they are not prudential supervisors or because they are not Financial Intelligence Units etc.

2. Non or partial cooperation between financial AML/CFT supervisors due to lack of an adequate framework to exchange confidential information

- For example, lack of legal framework in place to allow for exchange of confidential information, lack of MOU in place defining modalities for common AML/CFT inspections, etc…

3. AML/CFT issues are not always raised in the context of prudential supervisory cooperation: AML/CFT risks are often not put on the agenda until they have crystallised

- In some cases, effective mechanisms to facilitate the cooperation of prudential supervisors exist (for example supervisory prudential colleges), but AML/CFT

issues tend to be discussed mainly in relation to the prudential impact of fines for breaches of applicable AML/CFT obligations. There is little focus on preventative aspects of AML/CFT compliance and supervision. AML/CFT discussions are further hampered by the absence of specialist AML/CFT competent authorities who are not members of prudential colleges.

4. Non-transmission of relevant confidential information or refusal to communicate such information by a pure prudential supervisor (i.e. not in charge of AML/CFT) to an AML/CFT financial supervisor based on the argument of a lack of legal framework covering the legitimacy of such a transmission (which could lead to a violation of the legal supervisory confidentiality regime)

- Today, the ECB refuses to provide national AML/CFT supervisors with confidential prudential information that is also relevant for AML/CFT supervision (e.g. information on the fit and properness of directors or shareholders, information on the internal procedures for the management of compliance risks,..)

5. Non-cooperation or ineffective cooperation due to lack of clarity regarding the identity of the competent AML/CFT counterpart

- E.g. in some Member States, AML/CFT supervision is fragmented, with competent authorities organised by type of supervised entities, and/or type of supervisory action (for example for a certain type of FI, authority A is in charge of the licensing and authority B of the supervision). Therefore, supervisors may have problems to identify the relevant foreign counterpart in that country when looking to cooperate in relation to the AML/CFT supervision of a particular obliged entity.

Significant differences in supervisors' expectations and approaches are conducive to regulatory arbitrage (Joint Opinion ESAs)

The ESAs note that National Competent Authorities' (NCA) assessment of, and satisfaction with, their sectors' compliance with applicable AML/CFT rules varies significantly, including in cases where NCAs in different member states supervise entities that belong to the same financial group. This is due in part to:

a. continuing differences in NCAs' approach to AML/CFT supervision. NCAs who carried out in-depth thematic AML/CFT reviews tend to assess compliance levels more pessimistically than those who did not carry out such reviews;

b. the extent to which firms are already allowed to apply a risk-based approach, which determines the expectations NCAs have of their sectors' compliance with applicable AML/CFT obligations. NCAs tend to assess overall levels of AML/CFT compliance more pessimistically where they have more concerns

about their sectors' risk assessment than about the application of CDD measures; and

c. uncertainty about home/host supervisory responsibilities, in particular in relation to the AML/CFT supervision of payment institutions and their foreign agents (cf. overlap with the specific passporting issue below).

II. Passporting

Failure effectively to oversee agents and networks of agents for AML/CFT compliance purposes, in particular where agents are based in another Member State, risks leaving breaches or cases of abuse for financial crime purposes undetected (Joint Opinion ESAs). The underlying reasons can be the following:

1. Uncertainty about the home/host supervisory responsibilities (cf. supra, (c)).

2. The lack of consistent understanding and application of the EU "home/host" supervisory framework in relation to the AML/CFT oversight of agents established in another Member State. This gives rise to the increased risk of ML/TF which has the potential to undermine the robustness of Europe's AML/CFT defences.

3. Regulatory arbitrage: firms taking advantage of significant differences in Member States' approaches to AML/CFT regulation and oversight to obtain authorisation in Member States whose AML/CFT regime is perceived to be less demanding, with a view to passporting services to other Member States (Joint Opinion ESAs).

III. Supervisory means

Not all supervisors are sufficiently equipped to manage AML/CFT risks linked to new technologies (Joint Opinion ESAs)

New risks stem from technological developments and financial innovation. Firms and national competent authorities may not be well-equipped to identify and adequately supervise firms' management of these risks. Some financial institutions may struggle to adapt to a) new or innovative retail financial products, b) new payment methods or c) an increased "digitalisation" of services. This may hamper their ability to effectively identify, assess and mitigate ML/TF risks. On the other hand, new technologies may open up innovative avenues for how financial institutions meet their obligations; this may reduce costs and smooth the experience for customers.

Supervisors do not dedicate sufficient human and organizational resources to AML/CFT supervision of FI's, which undermines an effective supervision and sanctioning in the field of AML/CFT

MERs of the FATF and Moneyval have highlighted these risks and vulnerabilities in the case of a number of Member States.

Supervisors have insufficiently identified the AML/CFT risks linked to the sectors they supervise, and/or do not have risk based procedures in place to supervise these risks.

MERs of the FATF and Moneyval have highlighted these risks and vulnerabilities in the case of a number of Member States.

Also during the discussions/consultation on the ESAs joint opinion on the SNRA, it was confirmed that supervisors do not have sufficient understanding of ML/TF risks affecting the supervised sectors. This is even more acute concerning terrorist financing risks where supervisors were lacking awareness.

Mitigating measures

1) In addition to the sector specific recommendations, it is proposed that the ESAs:

- raise awareness on ML/TF risks and identify the appropriate actions to further build supervisors' capacity in AML/CFT supervision. In that context, they should carry out peer reviews on the application of the risk based supervision and identify suitable measures to increase effective application of AML/CFT supervision;

- take further initiatives to improve cooperation between supervisors. In this respect, the ESAs have recently decided to start a dedicated work stream in order to enhance the cooperation framework between financial supervisors;

- further work out solutions with regard to the issue of supervision concerning operators acting under the "passporting" regime. The EBA joint Task Force on payment services/anti-money laundering already started working on this issue. This joint task force aims at clarifying when agents and distributors are actual "establishments" and considering various scenarios that can be taken to address the risks;

- provide updated guidelines on internal governance further clarifying expectations with regard to the functions of compliance officers in financial institutions;

- provide further guidance on beneficial ownership identification for providers of investment funds, especially in situations presenting a higher risk of ML/TF;

- provide an analysis of operational AML/CFT risks linked to the business/business model in the corporate banking, private banking and institutional investment sector, as well as money value transfer services and e-money. Such analysis should be carried out in the context

of the future joint opinion on risks affecting the financial sector as mandated under article 6(5) of the 4AMLD;

2) as part of the enforcement work, specific focus will be put on assessing correct transposition of article 48 4AMLD as well as effectiveness of supervisory actions (based on MERs and annual review of statistics provided under art. 44, and encouraging the ESAs to carry out peer reviews on the application of guidelines under Article 48(10) of the AMLD);

Vulnerabilities linked to Financial Intelligence Units

Vulnerabilities linked to powers of Financial Intelligence Units, access to information and cooperation between FIUs in the EU

This description relates to horizontal vulnerabilities which were mentioned for different sectors regulated by 4AMLD. Where relevant the level of materiality of those vulnerabilities has been assessed in the respective product risk fiches. This paper covers only horizontal issues and possible mitigating measures of horizontal aspects.

Description of the vulnerability: EU FIUs may have uneven powers allowing them to access relevant financial, administrative and law enforcement information (especially those held by obliged entities and/or law enforcement authorities). There is a lack of available means in order to identify beneficial owners and holders of bank account within a jurisdiction. This may limit their operational capacity to carry out their intelligence functions and to reply to requests made by another EU FIU. Despite the integrated nature of the internal market, exchange of information between EU FIUs may be impeded – as well as the use and dissemination of information to competent authorities.

1. Analysis:

The EU FIU platform discussed those vulnerabilities and carried out a dedicated analysis. This "Mapping Exercise and Gap Analysis on FIUs' powers and obstacles for obtaining and exchanging information" (hereinafter: "Mapping Exercise") is aimed at identifying areas where further initiatives are needed to remove obstacles or remedy existing deficiencies. The report was adopted on 15 December 2016.

The report is based on the outcome of a thorough data collection exercise (comprehensive survey carried out in May 2016) and review process. Currently the cooperation framework for FIUs is still framed by the 3rd AMLD and the 2000/642 Council Decision on FIU which provide for limited harmonisation in this field. The 4AMLD reinforces FIU powers and entails very innovative features for EU FIU cooperation. However Member States did not yet implement the new provisions of the 4AMLD in this respect at the time of the analysis. In that context, the main findings of the mapping exercise are the following:

- the FIU status, powers, organisation, level of autonomy are considered as too uneven and not sufficiently harmonised at EU level. The main conclusion of the report is that the status and powers of FIUs significantly impact their ability to share information. Currently FIUs are organised in different ways (administrative, law enforcement, and hybrid FIUs). They have domestically different powers in accessing, sharing and using information – which therefore impact their capacity to cooperate with other EU FIUs. EU legislation only defines a limited set of requirements regarding the FIU status, powers and organisation and independence which does not ensure a similar level of authority among FIUs.

- FIUs do not have access the same level of information sources which hinders their capacity to share information (i.e. if they cannot access information because it does not exist / do not have an access right, they cannot exchange it with another EU FIU despite a legal obligation to share information). There is a requirement in 4AMLD that FIUs have access to administrative, financial and law enforcement information but in the absence of further clarification, the sources of information vary greatly between FIUs. FIUs still face limitations in accessing information held by obliged entities relating to ML/TF.

- The functions of FIUs are not sufficiently clear since there is often confusion between their intelligence function (regulated by 4AMLD) and their law enforcement function (support in police investigations). Since police FIUs are often directly involved in the investigation process, the intelligence and investigation stages are merged. Consequently they face limitations in cooperating with other FIUs (especially administrative FIUs), reverting instead to law enforcement / judicial cooperation tools which are unfit for FIUs working in the intelligence phase (i.e. pre-investigation stage).

- Concerning FIUs tasks, there is a lack of common understanding of "strategic analysis" as well as "operational analysis" to be provided by FIUs. Both tasks should be carried out by FIUs according to 4AMLD but in practice they do not have similar products (e.g. FIUs may only passively give access to their databases to police and support only investigations). There is also a lack of common approach for analysing cross-border cases in the EU internal market both at operational and strategic level.

- Sharing of information between EU FIUs remains challenging for many reasons. The first challenge consists in the lack of access to requested information. If FIUs do not have access to information domestically (e.g. it does not exist), they are de facto prevented from sharing it with another EU FIU. This may therefore trigger the "reciprocity conditions", i.e. the other EU FIU will not reply to a request for information if the requesting FIUs cannot share the same type of information for other cases. In addition, it was found that many FIUs still need a clearance from a third party to share information with another FIU for intelligence purposes (often police authority)– which may be refused or delayed without justified reasons. Another issue concerns the implementation of the new requirement in 4AMLD to share spontaneously an STR which concerns another Member States – for which FIUs are struggling to implement this in the absence of further definitions or common understanding. In addition, FIUs still apply limitations regarding the use and further dissemination of exchanged information for investigation purposes (which is nevertheless the ultimate goal of FIUs work). Such limitations are particularly frequent when the predicate crime is not identified in the initial request or not criminalised the same way in both countries (conditions of "double criminality") – or when it relates to tax offences ("fiscal excuse). Similarly such dissemination is refused in practice when there is an ongoing investigation or there are legal proceedings underway (irrespective of any risk of impairment of investigations). Those practices are in contradiction with the spirit of the 4AMLD, but its legal provisions are still vague.

- Data protection rules and dissemination rules are also uneven between EU FIUs. There is an uneven level of safeguards on data protection, security and confidentiality across

Member States, while EU rules are not detailed in that regard. FIUs also send the results of their analysis to different types of authorities, while the rules regarding the further use by those authorities are not sufficiently regulated. In particular the use that the receiving law enforcement authority can make is unclear; despite specific restrictions set by an FIU, some LEA/judicial authorities may consider received information as formal "evidence" according to their judicial system. To avoid such risks, some FIUs may simply refuse the sharing with another FIU or prohibit dissemination to another authority - instead of giving its consent with specific restrictions. Hence it is proposed that FIUs should receive "a priori" the consent for sharing the information with law enforcement authorities for intelligence purposes only – while ensuring that law enforcement authorities/judicial authorities revert to LEA/judicial cooperation instruments for using this information for evidentiary purposes.

2. Mitigation measures

- The 4AMLD will further specify the tasks of FIUs and provide for a new regime for cooperation between FIUs in the EU. Effective implementation of 4AMLD will be essential for addressing key deficiencies.

- In addition, the Commission proposed to revise the 4AMLD in order to increase the effectiveness of FIUs by setting up centralised bank account registers or retrieval systems which will allow better targeted requests. Access to information held by obliged entities by FIUs will also be facilitated, in line with international standards. With this approach, FIUs will have a minimum common set of information sources (i.e. STRs, information held by obliged entities, registers on beneficial ownership information and bank account registers).Finally provisions on FIU cooperation will be further upgraded to ensure information sharing without impediments caused by the "dual criminality principle" or "fiscal excuse".

- The Commission will further examine potential options in line with its Better Regulation principles. Possible avenues are outlined in the Staff working Document on FIU cooperation.

ANNEX 2 – PROJECT CHARTER

DG JUSTICE AND CONSUMERS
Unit A3 Company law

Project Charter

[Subject]

Inspired by

Date: 200 / 290

Doc. Version:

TABLE OF CONTENTS

1 Executive Summary 1-1

2 Project Objectives 2-1

3 Project Description 3-1

3.1 Scope 3-1

3.1.1 Scope Statement 3-1

3.1.2 Work Items ("WI" Scope) 3-1

3.1.3 Out-Items ("OI" Scope) 3-1

3.2 Technical Criteria 3-2

3.3 Stakeholder and Asset Needs 3-2

3.4 Deliverables (Outputs) 3-3

3.5 Outcomes 3-4

3.6 Constraints 3-5

3.7 Assumptions 3-5

3.8 Risks 3-6

4 Work, Timing, and Resources 4-1

4.1 Work Tasks, Interfaces 4-1

4.2 Timing, and Milestones 4-1

5 Assessment and Stakeholders 5-1

5.1 Key Facts 5-1

5.2 Roles and Responsibilities 5-2

5.3 Other Stakeholders 5-3

1 Executive Summary

The purpose of this Charter is to document the management of the described project. As part of the success factor, it is considered as necessary to clarify the scope of the project, its resources (time, budget, staff), and the governance (who does what?). This information trail should also allow explaining to external users how the Commission conducted this project. This Charter was developed by considering the Commission's methodology for project management (PM²).

The objective of the project is to carry out an EU assessment on the money laundering (ML) and terrorist financing (TF) risks as provided in the Directive (EU) 2015/849 (also referred to as "EU Supranational Risk Assessment on AML/CFT –"SNRA"). The project will take place in 2 phases:

1) **Risk analysis phase:** the objective of this phase is to identify and analyse money laundering and terrorist financing risks - a risk being identified as the ability of a threat to exploit vulnerability of a given sector for the purpose of perpetrating ML/TF. This phase will be carried out in accordance with a specific methodology (see annex6). For each identified ML/TF scenario that will be identified, the Commission will assess the level of threat and the vulnerability of the sectors thus allowing to rate the level of risk.
2) **Risk mitigation phase**: the objective of this phase is to define mitigating measures to address the identified risks. These mitigating measures will include Recommendations to Member States.

In order to ensure collective ownership and coordination between Commission Services, the Inter-Service Group on AML/CFT will act as steering committee during this project. The risk analysis will be carried by a Project team within the Commission (JUST.A3 and HOME.D1.03). The risk analysis will be defined through a series of Workshops involving Commission Services, Europol, the European Supervisory Authorities, and Member States' experts.

JUST.A3 is ultimately accountable and responsible for the SNRA project.
HOME.D1.03 ("Strategic analysis and response") is providing services to JUST.A3 in the risk analysis phase.

In terms of results, this will lead to the adoption of an SNRA report by 26 June 2017. This deliverable will consist of a:
- Communication from the Commission presenting the key risks and the proposed mitigating measures (including Recommendations to Member States);
- a Staff working document providing a more comprehensive factual and informative description of the risk assessment;
- classified annexes to protect sensitive information (if necessary).

2 Project objectives

The objective of the project is to carry out an EU assessment on the money laundering and terrorist financing risks as provided in the Directive (EU) 2015/849 ("SNRA").

Article 6 of the 4th AML Directive foresees that the Commission shall conduct an assessment on the money laundering and terrorist financing risks affecting the internal market and related to cross-border activities (see Annex 1). To that end, the Commission shall draw up a report identifying, analysing and evaluating these risks at Union level. The outcomes of the risk assessment will inform the Commission which is responsible for defining the measures suitable for addressing and mitigating the identified risks including recommendations to Member States.

The 4th AML Directive provides that Union actions in this field should, where appropriate, be aligned with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation adopted by the FATF in February 2012 (the 'revised FATF Recommendations'). Hence the project aims at following the standards defined by FATF as well as the guidelines established in its document "FATF Guidance – National Money Laundering and Terrorist Financing Risk Assessment" (February 2013).

3 Project Description

3.1 Scope

3.1.1 Scope Statement

The overall scope is to assess the money laundering and terrorist financing risks affecting the internal market and related to cross-border activities. The EU SNRA is carried out in line with the FATF Recommendation No 1 and its Interpretative Note (see Annex 2). The aim is to identify, assess and understand the ML/TF risks affecting the EU internal market and to take actions in order to ensure that risks are effectively mitigated.

3.1.2 Includes ("IN" Scope)

The scope covers the following phases:

Phase 1: Risk analysis:

- Identification of the risks: the process of identification aims at developing a list of risks

- Analysis of the risk: the process of analysing aims at understanding the nature and level of the risks

Phase 2: Mitigation/evaluation phase:

- The evaluation of risks leads to the identification of mitigation measures to address the identified residual risks.

According to the provisions of Directive (EU) 2015/849 (so called 4th AMLD – "4AMLD"), the risk assessment should cover at least the following:
(a) the areas of the internal market that are at greatest risk;
(b) the risks associated with each relevant sector;
(c) the most widespread means used by criminals by which to launder illicit proceeds.

The project aims at capturing both current known risks, as well as new and emerging risks. Besides this, the scope of the EU SNRA should specifically cover the following elements:

- assess the risks posed by gambling services as provided in article 2(2) of the 4AMLD (see Annex 2)

- money laundering as well as terrorism financing risks, with a focus on the latter (as demanded by the Council and the Commission – see Annex 3)

- assess the risks posed by virtual currencies (as demanded by the Council and the Commission - see Annex 3)

3.1.3 Excludes ("OUT" Scope)

The 4AMLD provides for 3 levels of assessment (supranational level, national level, obliged entity level) – without prescribing how the SNRA shall consider the results of the NRAs.

The scope of the SNRA does not cover a systematic compilation of the National Risk Assessment (NRA) carried out by Member States according to Article 7 of the 4AMLD. This is due to the fact that Member States have reached an uneven stage for preparing their NRAs. Different methodologies are used at national level which makes any compilation of the results impossible at this stage of development. This scope exclusion may be reassessed in the future once Member States will have reached more similarity in developing their NRAs.

3.2 Success Criteria

The success of the EU SNRA exercise will depend on the following key factors:

- Commitment of Member States' experts to contribute to the SNRA exercise.
- Involvement of Commission's Directorate Generals to ensure coherency, consistency and collective ownership of the exercise.

- Availability of resources to carry out the exercise (in the Commission, EU agencies and Member States).
- Regular communication on SNRA work in progress and results with stakeholders (public and private sector).
- Mutual trust between contributors in exchanging information
- Transparency of the SNRA process/outcome while at the same time ensuring strict confidentiality regarding exchange of sensitive information.
- Involvement of the intelligence community in particular the analysis of EU Intelligence Analysis Centre (INCENT)
- Protection of classified information

3.3 Stakeholder and User Needs

The main stakeholders and users are set in article 6(3) of the 4th AML Directive. The project shall take into account the need of key stakeholders and users of the SNRA which are typically EU institutions, Member States, obliged entities (private sector), international community, Academics, NGO and the public.

ID	Stakeholders	Need Description	Priority (L, M, H)
N1	***European Institutions***	EU institutions and agencies (such as European Supervisory Authorities) need an evidence based analysis in order to understand, evaluate and mitigate the risks by developing policy initiatives in accordance with the identified level of risks.	High
N2	***Member States (MS)***	MS need to understand the risks affecting the EU internal market and related to cross border activities. MS make use of the SNRA findings when carrying out the national risk assessments (art.7 of the Directive). MS shall understand the risks in order to implement Recommendations issued by the Commission on a "comply or explain basis" (art. 6 of the Directive).	High
N3	***Obliged entities (private sector)***	Obliged entities need to understand the risks affecting the EU internal market and related to cross border activities when carrying out their entity's risk assessment (art. 8 of the Directive)	Medium
N4	***International community***	FATF, FATF-Style Regional Bodies, and third countries have an interest in understanding the risks affecting the EU internal market and related to cross border activities in order to identify best practices, implement the risk-based approach and develop appropriate policy initiatives.	Medium
N5	***Academics, NGO and public***	Academics, NGO and the general public have an interest in understanding the risks affecting the EU internal market and related to cross border activities and the policy response to address the identified risks.	Low

3.4 Deliverables (output)

The project aims at delivering a Communication from the Commission, supplemented by a staff working document. Technical annexes may contain classified/confidential information.

ID	Deliverable Name	Deliverable Description
D1	*Commission Communication on the money laundering and terrorist financing risks affecting the internal market and related to cross-border activities*	This document will be adopted by the Commission . It presents the main findings regarding the identification, analysis and evaluation of ML/TF risks. It includes the mitigating measures considered as appropriate to address the risks. It is limited to 15 pages.
D2	*Staff working document*	This document complements the Communication by providing a more comprehensive factual and informative description of the risk assessment. It does not have any legal effect and does not commit the European Commission.
D3	*Confidential annexes (if necessary)*	This document contains the information relating to the risk assessment which is sensitive enough to need classifying and therefore protection for a short or long period of time. If this information was revealed prematurely or was obtained by the wrong persons, damage could be caused to the interests of the Commission, EU or Member States to varying degrees.

3.5 Features

The deliverables should meet the needs of the different stakeholders by having the following features:

ID	Related Need	Feature	Description
F1	*N1, N2, N3, N4, N5*	*Evidence based*	The deliverables shall be based on evidence and review of available statistical data.
F2	*N1, N2, N3, N4, N5*	*Due process*	The deliverables are the results of a due process based on a recognised methodology and the feedback collection of all relevant stakeholders
F3	*N1, N2, N3, N4, N5*	*Descriptive analysis*	The deliverables shall contain a descriptive analysis in order to allow users to understand the relevant risks being analysed. The Staff working document shall be sufficiently detailed in order to allow understanding the specific risks.
F4	*N1, N2, N3, N4, N5*	*Mitigating measures*	The Communication shall clearly set the mitigating measures to address the risks and explain why they are necessary.
F5	*N1, N2, N3, N4, N5*	*Communication tool*	The SNRA shall be used as a communication tool in order to present the EU expertise in analysing ML/TF risks, the EU commitment for tackling seriously this issue and promote our forefront activities in this policy field.

F6	*N1, N2*	*Protected*	Information considered as sensitive needs to be protected adequately throughout the process – including in the publication of deliverables.

3.6 Constraints

The following constraints are being imposed to the project:

- Delivery of the SNRA report within 2 years after entry into force of the 4AMLD (25 June 2017)
- Subsequent updating delivered every 2 years (or more frequently if appropriate)
- Resources available (see section on resource definition)
- Relying on Member States and EU agencies expertise and data for carrying out the SNRA
- Security constraints in order to protect sensitive information from criminal groups/terrorists.

3.7 Assumptions

It is assumed that:

- DG HOME (unit D1. Strategic analysis and response) provides the required support for the SNRA exercise during the risk analysis phase
- The European Supervisory Authorities deliver their joint opinion by the due date (26 December 2016) with an adequate level of quality in order to assess the vulnerability of the financial sector
- Member States' experts are delivering the expected input on time and with the required level of quality.
- DG JUST allocates the planned resources (i.e. staff) for carrying out this project. Assigned staff are able to focus on the project without major disruption caused by new/emerging demands.

3.8 Risks

In line with the Commission's risk management framework (SEC(2005)1327), the different risks related to the project should be properly identified, understood and mitigated. A risk is defined as any possible event that may jeopardise the achievement of the project's objectives (i.e. even if the risk did not yet materialise). The following main risks have been identified and addressed:

ID	Risk Description & Details	Risk level	Risk Response Strategy[20]	Mitigating actions
R1	*Users may criticise the results/outcome of the SNRA, thus questioning the EU framework and relevance of proposed mitigating actions.*	High	Reduce	The Commission develops the SNRA based on a pre-agreed methodology. The methodology closely follows best practices and guidance provided by FATF (INR1). The methodology is applied through a holistic approach allowing the different stakeholders to contribute to the exercise. The analysis is based on quantitative and qualitative information.
R2	*The Commission may not have the intelligence or information in order to deliver the required input into this exercise*	Low	Share/ Transfer	The process shall involve Commission services, IntCen, EU agencies (Europol, European Supervisory authorities) and MS authorities. Consultation process of private sector and NGOs take place to collect further information. Holistic approach ensures that knowledge and information is collectively available.
R3	*Member States may not share information because it is considered as too sensitive or information is classified. There is a lack of trust thus hindering Member States to exchange information.*	Medium	Reduce	Transparency and due process are ensured during the process in order to create trust among experts. In addition, security arrangements are set up in order to protect sensitive information. Confidential information is classified and, where appropriate, discussions are held in a secure zone. Participants of classified meetings – including Commission staff - have a proper and valid security clearance.
R4	*DG JUST may not have the required expertise to carry out a ML/TF risk assessment, especially for the threat assessment. The expectations between the contributing services, especially DG HOME may not be clear and lead to unclear task allocation impeding the project.*	Medium	Reduce	The methodology to be developed is inspired by those from Member States NRAs. DG HOME ("Strategic analysis and response") is delivering support based on its experience with security related risk assessments. DG JUST and HOME prepared jointly the methodology and the project charter in order to have a common vision. The project charter clarifies the roles and responsibilities, as well as the needed resources.

[20] The possible risk response strategies are: Avoid/ Transfer or Share/ Reduce / Accept.

ID	Risk Description & Details	Risk level	Risk Response Strategy[20]	Mitigating actions
R5	*There may be a lack of statistical information to support the analysis. Data may be owned by Member States using different definitions and collection methods. There may be limited data available and when they exist, data may not be comparable or may not be reconciled.*	Medium	Accept	4AMLD requires MS to deliver statistical information to the Commission. Data gathering will be facilitated after transposition of the Directive and development of NRAs.
R6	*There may be a lack of ownership of other Commission services. They may not be contributing/involved in the SNRA process or do not have a chance to deliver input. The results of the SNRA may be considered as a DG JUST product and other services do not feel bound by the conclusions. Ultimately, the SNRA report may be blocked or deteriorated during the Interservice consultation, thus failing to produce the report on time.*	High	Reduce	An inter-service group on AML/CFT (ISG AML) is set up within the Commission. The ISG is composed of all DGs having a policy interest in AML/CFT, including corporate DGs (SG and SJ). The ISG will act as steering group in order to facilitate the process, ensure collective ownership and allow early input of COM services into the process.
R7	*Member States are delivering limited input during the process. The right people having the information are not attending the workshops. Numerous MS experts are attending the meeting in a passive way as observer, thus representing a logistical and operational challenge.*	High	Accept + reduce	Clear instructions regarding the number of allowed experts will be communicated to Member States. Emphasis will be put on the operational aspect of such meetings (and not institutional ones), requiring a high level of information and expertise from participants. Workshops are prepared well in advance by developing background/discussion papers. ISG, EGMLTF and FIU platform members are requested to prepare analytical fiches.
R8	*Risks may change during the course of the SNRA project or new risks may emerge without being considered. The analysis may be outdated or not addressing actual risks at the moment of publication*	Low	Reduce	The scope of the SNRA explicitly covers known and emerging risks. The Commission will consider possible emerging risks as part of the risk universe in the risk identification phase. The likelihood of major changes in the vulnerability is low – since the residual vulnerability is linked to the control environment which is rather predictable. In case there is nevertheless a major change during the course of the SNRA, the Commission retains its decisionary power to update the risk analysis at any moment. Hence the Commission can always adapt

ID	Risk Description & Details	Risk level	Risk Response Strategy[20]	Mitigating actions
				its risk analysis during the course of the analysis to take into account of latest developments.

4 Cost, Timing and Resources

4.1 Cost and resources

The SNRA report will be prepared by using Commission resources ("in-house report"). Hence there is no need to provide for an operational budget.

1. Staffing/resources:

- JUST.A3 will dedicate approximately 530 man days (1,1 Full Time Equivalent - FTE/year) over the 2,5 years needed for developing the first SNRA report (Jan 2015-July 2017).

- HOME.D1 – strategic analysis and response – will support the process by providing methodological guidance, logistical support and facilitation services in view of the workshops. It will dedicate approximately 100 man days to this project.

- Other Commission services: other Commission services (HOME, TAXUD, FISMA, FPI etc.) will be involved during the process depending on the needs. The involvement is considered as non-material in quantitative terms (total of approximately 60 man days based on the number of restricted ISG meetings). It is part of the usual horizontal coordination process in this policy field. Hence the allocated resources are not further assessed.

Experts attending the workshops are self-financing their participation. There is no specific operational budget allocated for paying participation of experts. Depending on the availability, reimbursement for some meetings may take place (administrative budget).

2. Other resources

During the project, the project team will need the following resources:

- meeting room (capacity of 80 persons)

- use/access to a secure zone for exchanging confidential information

- valid security clearance for project team members

4.2 Timing and Milestones

This section lists the important project points in time of the project lifecycle (i.e. milestones) for the project. This list is complemented by a Gantt Chart (annex 4), a workflow (annex 5) as well as the SNRA methodology (annex 6).

ID	Milestone Description	Target Delivery Date
M1	**Initiating and Planning:** The aim is to develop the SNRA methodology to be applied during the process.	**End of October 2015**
M2	**Executing: Risk identification ("identify")** The aim is to identify a list of risks/modi operandi of money laundering and terrorist financing. A risk is defined as the ability of a threat to exploit vulnerability of a given sector for the purpose of perpetrating ML/TF.	**End of February 2016**
M3	**Executing: Threat Assessment phase ("Analyse")** The aim is to assess the level of threat for each ML/TF modus operandi. A threat is defined as a person/group with the potential to cause harm to the state, society, the economy. The level of threat will be assessed depending on the intent and capability of criminals/terrorists of using the modi operandi	**End of April 2016**
M4	**Executing: Vulnerability Assessment phase ("Analyse")** The aim is to assess the vulnerability of the different sectors that may be exploited by criminals/terrorist. The level of vulnerability will assess the residual level considering the inherent vulnerability of the sector and the control systems in put in place to prevent an occurence.	**End of July 2016**
M5	**Executing: Consolidation ("Analyse")** The aim is to consolidate the threat and vulnerability assessment in order to define the risk level.	**End of October 2016**
M6	**Risk management ("Evaluate/mitigate")** The aim is to manage the identified risks and develop a risk response (refuse, reduce, transfer, accept). The end-result will consist in an identification of mitigating measures to address the risks. This is followed by an action plan which serves as the basis for the COM Communication	**By March 2017**

ID	Milestone Description	Target Delivery Date
M7	**Formal approval** The aim is to formally approve the deliverables by the College of Commissioners in line with Commission rules.	**By June 2017**
M8	**Closing** The project is formally closed. A post-mortem meeting takes place with the project managers, AML team leader and HOME.D1 in order to review lessons learnt. A short closing document is prepared to summarise strength, weaknesses and lessons learnt during the project. The closing document, the project charter and the SNRA methodology are handed to the policy officer in charge of future updates.	**By September 2017**

5 Governance and Stakeholders

5.1 Structure

The project structure will be composed of an Interservice group and a Project Team. In the following section, the roles of key project members and stakeholders are described alongside with their responsibilities.

- *Steering Committee*

Name	Interservice Group
Description	The Interservice group on AML/CFT (ISG) will act as Steering Committee. It is composed of DGs having an interest in AML/CFT policies. In the context of the SNRA, the ISG consists at least of the following permanent members: Chair: Head of Unit – JUST.A3 Members JUST.A3 – AML Team HOME.D1.03 – Service provider (SP) HOME.D1.01 – counter terrorism: prevention HOME.D2 – fight against organised crime TAXUD.B1 – cash control FISMA coordinator on AML (FISMA.02) FISMA D.3 - Retail financial services/Payment GROW E.2 - Gambling EEAS VI.B – Gobal issues and counter terrorism ECFIN.DDG1.C.5 Euro protection and euro cash among the members Secretariat General (SG) – SG.E1 Legal Service (LS)
Responsibilities	⁄ Champions the project, raising awareness at senior level. ⁄ Guides and promotes the successful execution of the project at a strategic level. ⁄ Provides high level monitor and control of the project. ⁄ Authorises plan deviations, scope changes with high project impact and ensures coherency with Commission policies ⁄ Arbitrates on conflicts and negotiates solutions to important problems. ⁄ Ensures consistency and adherence to organisation policies and directions. ⁄ Approves and signs-off all key management documents (Project Charter, Methodology, Project Work Plan. etc). ⁄ Approves and signs-off all key project deliverables

- *Project Team*

Name	SNRA Project Team
Description	The SNRA project team (PT) consists of the roles responsible for the implementation of the project. It is led by the AML Team Leader and is composed of: • AML Team Leader • Business Manager (JUST.A3) • Project Manager (JUST.A3) • Service Provider (HOME.D1.03)
Responsibilities	Under the coordination of the AML Team Leader, the SNRA Project Team (PT): • Contributes in the elaboration of the project scope and the planning of the project activities. • Performs the project activities according to the project work plan and schedule. • Provides information to the AML team leader regarding the progress of activities. • Participates in resolution of issues. • Participates in the Project-End Meeting to derive and document useful lessons learned for the organisation.

5.2 Roles and Responsibilities

This section lists the roles and responsibilities of the key staff involved in the SNRA project. The project is covering two phases: 1) the risk analysis phase and 2) the risk mitigation phase. As Project owner, JUST.A3 is ultimately accountable and responsible for the successful carrying out of the 2 phases. The services delivered by HOME.D1 as Service Provider is limited to the first phase (risk analysis only).

Roles	Short Description
Project Owner (PO)	**Head of Unit JUST.A3** Ultimately accountable for the overall SNRA project: ▪ Acts as the project champion promoting its success. ▪ Chairs the Steering Committee (Inter-Service Group). ▪ Sets the business objective for the project and ensures that the project outcome meets business expectations. ▪ Owns the project risks and assures proper project outcomes are in-line with business objectives and priorities. ▪ Mobilises the necessary resources for the project in accordance to the budget. ▪ Monitors project progress regularly. ▪ Provides leadership and strategic direction to the Business Manager and Project Manager ▪ Coordinates resolution of issues and conflicts. ▪ Approves and signs-off all key management documents (Project Charter, SNRA methodology).
Business Manager (BM)	**JUST.A3** Represents the Project Owner: ▪ Assists the Project Owner (PO) on the specification of the project and the main business objectives. ▪ Manages the business side activities of the project – for both 1) the risk analysis phase and 2) the risk mitigation phase. ▪ Contributes to the deliverables from a business/ policy perspective ▪ Delivers input to the Project Manager and the Service Provider from a business / policy perspective ▪ Ensure that the deliverables and outcomes are in-line with business objectives and priorities

Roles	Short Description
Project Manager (PM)	**JUST.A3** Responsible for the whole project and its deliverable regarding both 1) the risk analysis phase and 2) the risk mitigation phase. Assumes responsibility for the final project deliverables: ▪ Establishes and guarantees an efficient collaboration and communication channel with the Service Provider. ▪ Ensures that all key management milestone documents are delivered and approved by the Project Owner (PO). ▪ Communicates and reports project progress to the Steering Committee (ISG). ▪ Proposes and executes the project plans as approved by the Interservice Group ▪ Ensures that project objectives and deliverables are achieved within the quality, time, and cost objectives
Service Provider (SP)	**Head of Sector – HOME.D1.03** Assumes the accountability for project deliverables and services requested by the Project Owner (PO) in the risk analysis phase. ▪ Helps the Project Owner (PO) in defining the Methodology and objectives for the project. ▪ Represents the interests of those designing, delivering, procuring, and implementing the project's deliverables. ▪ Mobilises the needed resources from the supplier side. ▪ Is responsible for delivering the requested services within the quality, time, and cost objectives NB: The Project Manager is not providing any support in the risk mitigation phase.

5.3 Other Stakeholders groups

- *SNRA Workshop*

Name	SNRA Workshops
Description	The SNRA workshops will assist the Commission in carrying out the risk identification and risk analysis through a series of meetings in accordance with the SNRA methodology. It is composed of the following experts:

Name	SNRA Workshops
	Chair: European Commission (JUST.A3) Service Provider: European Commission (HOME.D1.03) Members: Member States experts on AML/CFT (28MS)* Europol European Supervisory Authorities (ESAS) Relevant Commission services (policy level) * Member States are responsible for nominating the suitable experts for the different workshops during the SNRA exercise
Responsabilities	✓ Identify ML/TF modi operandi that will be further assessed during the SNRA project ✓ Assess the level of threat of each modus operandi ✓ Assess the level of vulnerability for each modus operandi ✓ Review the outcome following the establishment of the risk matrix

EGMLTF

Name	EGMLTF
Description	EGMLTF is permanent Commission expert group composed of Member States experts on ML/TF with the mandate of assisting the Commission e.g. in the preparation of policy definition and providing expertise to the Commission when preparing implementing measures.
Responsabilities	✓ Nominate suitable experts for the different workshops ✓ Prepare background information in view of the different workshops in line with the SNRA methodology (need basis) ✓ Deliver feedback in the preparation of policy definitions

- *FIU platform*

Name	FIU platform
Description	FIU platform is a permanent Commission expert group composed of Member States Financial Intelligence Units (FIUs). Its role is to provide advice and expertise to the Commission on operational issues in the context of the functions performed by FIUs. It also discuss trends and factors relevant to assessing money laundering and terrorist financing risks both on the national and supranational level.
Responsabilities	⁄ Prepare background information in view of the different workshops in line with the SNRA methodology ⁄ Deliver feedback in the preparation of policy definitions

- *Private Sector*

Name	Private sector and civil society consultative meetings
Description	The private sector consultative meeting allows the Commission to involve obliged entities in the conduct of the SNRA. The civil society consultative meeting allows the Commission to involve Non-Governmental Organisations (NGOs) and Academics in the conduct of the SNRA.
Responsabilities	⁄ Deliver feedback on the risks and modi operandi to be covered by the SNRA ⁄ Deliver feedback on suitable mitigation measures to address identified risks ⁄ Raise awareness and communicate SNRA issues to their membership basis.

- *Ad how working group (methodology)*

Name	Ad hoc working group
Description	The Ad hoc working group will support the development of the methodology for carrying out the identification, assessment and evaluation of the supranational ML/TF risks. It is composed of the following experts: Chair: European Commission (DG JUST) Project Manager: European Commission (HOME.D1.03) Members Volunteers from EGMLTF and FIU platform, Europol, European Supervisory Authorities
Responsabilities	⁄ Support the development of the SNRA methodology ⁄ Support on methodological implementation issues and changes in case of need.

- *European Supervisory Authorities*

Name	European Supervisory Authorities
Description	The European Supervisory Authorities (ESAs) are composed of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA). They are tasked with issuing an opinion, through their Joint Committee, on the risks affecting the Union financial sector. The opinion of the Joint Committee is prepared by the AML Committee of the ESAs (AMLC).
Responsabilities	⟋ Deliver a joint opinion on risks affecting the Union financial sector ⟋ Contribute to the development of the SNRA methodology in the ad hoc working group. ⟋ Contribute to the SNRAs workshops.

- - - ooo - - -

Annexe 1. Provisions of article 6 of the 4th AML Directive

Article 6

1. The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

2. The report referred to in paragraph 1 shall cover at least the following:

   (a) the areas of the internal market that are at greatest risk;

   (b) the risks associated with each relevant sector;

   (c) the most widespread means used by criminals by which to launder illicit proceeds.

3. The Commission shall make the report referred to in paragraph 1 available to the Member States and obliged entities in order to assist them to identify, understand, manage and mitigate the risk of money laundering and terrorist financing, and to allow other stakeholders, including national legislators, the European Parliament, the ESAs, and representatives from FIUs to better understand the risks.

4. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In the event that Member States decide not to apply any of the recommendations in their national AML/ CFT regimes, they shall notify the Commission thereof and provide a justification for such a decision.

5. By 26 December 2016, the ESAs, through the Joint Committee, shall issue an opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector (the 'joint opinion'). Thereafter, the ESAs, through the Joint Committee, shall issue an opinion every two years.

6. In conducting the assessment referred to in paragraph 1, the Commission shall organise the work at Union level, shall take into account the joint opinions referred to in paragraph 5 and shall involve the Member States' experts in the area of AML/CFT, representatives from FIUs and other Union level bodies where appropriate. The Commission shall make the joint opinions available to the Member States and obliged entities in order to assist them to identify, manage and mitigate the risk of money laundering and terrorist financing.

7. Every two years, or more frequently if appropriate, the Commission shall submit a report to the European Parliament and to the Council on the findings resulting from the regular risk assessments and the action taken based on those findings.

Annexe 2. Provisions of article 2(2) of the 4th AML Directive

Article 2

2. With the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

   Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

   In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6.

   Any decision taken by a Member State pursuant to the first subparagraph shall be notified to the Commission, together with a justification based on the specific risk assessment. The Commission shall communicate that decision to the other Member States.

Annexe 3. Declarations of the Commission and the Council of 27 January 2015

JOINT DECLARATION OF THE COMMISSION AND THE COUNCIL

IN THE CONTEXT OF THE ENDORSEMENT

OF THE ANTI-MONEY LAUNDERING (AML) PACKAGE

1/ The recent attacks in Paris have demonstrated the need to take decisive actions against terrorist financing. The adoption of the 4th Anti-Money Laundering Directive and of the Regulation on the Information Accompanying Transfers of Funds, which are strategic texts for the European Union, represent a significant step towards improved effectiveness in this fight.

2/ To enhance the efficiency of the new rules brought by this package, further efforts should be promoted, notably towards:

i) Speeding up the process of national implementation of those rules;

ii) Further strengthening cooperation on terrorist financing between Financial Intelligence Units at European level (for example through the work of European fora such as the FIU Platform);

iii) Addressing terrorist financing risks via the EU's supranational risk assessment, which should notably also assess the risks posed by virtual currencies;

3/ It is of utmost importance that coordinated action at international, European and national level to tackle terrorist financing is as effective as possible. Council and Commission will be examining further actions on countering terrorist financing in the context of the upcoming European agenda on security. A first discussion on this is expected to take place at the informal meeting of the European Council on 12 February.

Annex 4: Gantt chart (see separate file)

Annex 5: Project Workflow (see separate file)

Annex 6: SNRA Methodology (see separate file)

ANNEX 3 – METHODOLOGY FOR THE SUPRANATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS

Approved at ISG AML/CFT
Date: 04.11.2015
Version 1.1

Methodology

for assessing money laundering and terrorist financing risks affecting the internal market and related to cross-border activities

A risk means the ability of a threat to exploit the vulnerability of a sector for the purpose of money laundering or terrorist financing. A risk falls within the scope of this assessment as soon as it affects the internal market because of its characteristics – whatever the number of MS concerned (i.e. even if it may concern only one Member State). The scope covers both known and emerging risks – i.e. whether the risk materialised or not.

1. INTRODUCTION

The Financial Action Task Force (FATF) recommends that countries shall consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of each sector submitted to AML/CFT requirements when they decide to conduct a risk assessment. Money laundering (ML) and terrorist financing (TF) risks shall be identified, assessed and understood, and measures to prevent ML/TF shall be commensurate with the risks identified.

On the basis of these recommendations, the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[21] recognises the importance of a supranational approach to risk identification. It tasks the Commission to conduct the review of specific risks that could arise at European level and could affect the internal market ("supranational risk"). The Commission shall therefore conduct such Supranational Risk Assessment on money laundering and terrorist financing ("SNRA"). A risk identification is also conducted at national level by each Member States so that to ensure proper risk identification and risk mitigation of national specific risks. A third layer of risk identification is provided by sectors themselves, taking into account risk factors including those relating to their customers, countries, products, services, transactions or delivery channels.

These three layers of risk assessments (and where appropriate risk mitigation) allow building a comprehensive awareness and analysis of ML/TF risks in the European Union. There are complementary and have the same level of relevance as regards, respectively, the sectorial, national and supranational approach to the risk assessment.

Even though national and sectorial risk assessments, among other sources, may prove to be essential building blocks for the SNRA conducted by the Commission, it cannot be considered as a mere compilation of these ones. The SNRA exercise shall therefore be understood as a separate work stream. This is a pre-requisite for an efficient exercise consistent with the mandate of the Directive (EU) 2015/849, especially when the Commission will make recommendations to Member States on the measures suitable for addressing the

[21] O.J. L.141, 5.06.2015, p.73

identified European ML/TF risks. In carrying out the national risk assessments, Member States shall also make use of the findings of the SNRA report.

2. SCOPE AND OBJECTIVE

The aim of this document is to define methodological guidelines, governance, working arrangements and road map in order to support the conduct of the risk assessment and the interactions with relevant stakeholders in terms of inputs, expertise and advice.

The objective and scope of the risk assessment is defined in article 6 of Directive (EU) 2015/849 (see annex 3 for the provisions of the Directive). For the purpose of this methodology, the objective is to carry out an **assessment of supranational ML/TF risks** (see annex 4 for the definitions).

The "evaluation" of the identified and assessed risks (outcomes of the risk assessment) is out of the scope of these methodological guidelines and shall be considered within the framework of the overall risk management process leading to the identification of mitigation measures to fill the identified residual risks (see annex 2).

3. ROLES AND RESPONSIBILITIES ON EU SUPRANATIONAL RISK ASSESSMENT

3.1. ROLE OF THE COMMISSION

Following the mandate given by Article 6 of the Directive (EU) 2015/849, the Commission is responsible for drawing up the SNRA report and for defining the mitigating measures.

The Commission will conduct the assessment by:
- organising the work at European level and involving the appropriate experts;
- making the joint opinions of the European Supervisory Authorities (ESAs) as well as the SNRA report available to the Member States and obliged entities;
- defining the mitigating measures, making recommendations to Member States on the measures suitable for addressing the identified risks.

In that context, though the Commission will rely on the expertise of several stakeholders (see point 3.3), **it will have a decisional power to validate the outcomes of the SNRA discussions**.

An Inter-service Group of the Commission will act as steering group for this exercise.

3.2. ROLE OF THE AD HOC WORKING GROUP

In order to define a risk assessment methodology, an Ad Hoc Working Group (ADHWG) composed by volunteers from Member States has been set up in February 2014. The role of the ADHWG is to support the development of the methodology for carrying out the identification, assessment and evaluation of the supranational ML/TF risks as provided for in the Directive (EU) 2015/849. The ADHWG will follow the approach defined by FATF in its "Guidance on National Money Laundering and Terrorist Financing Risk Assessment" published on February 2013[22]. Following the finalisation of the methodology, the ADHWG will be consulted on methodological implementation issues and changes in case of need.

3.3. ROLE OF OTHER STAKEHOLDERS

During each step of the process, the Commission will involve the relevant experts from Member States[23] and European bodies as defined in the Directive. Where appropriate, the Commission will also involve representatives from the private sector, NGOs or academics in the process. Input and relevant information could be requested to the following stakeholders through ad hoc processes (public consultation, questionnaires, preparation of background papers, bilateral meetings…):

Experts group on money laundering and terrorist financing (EGMLTF): EGMLTF is a permanent Commission expert group composed of national administrations with the mandate of assisting the Commission, e.g. in the preparation of policy definition and providing

[22] see http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

[23] Throughout this document, indications about the composition of the Member States experts groups designated to conduct the risk identification and risk assessment are provided for sake of information. However, the appointment of the most relevant experts is left to the appreciation of each Member States by considering the specific expertise required for each dedicated phase of the risk identification and assessment. It may include representatives of supervisory authorities, financial intelligence units, customs, gambling sectors, ministerial authorities, law enforcement, etc…

expertise to the Commission when preparing implementing measures. EGMLTF has the capacity to draw on expertise available nationally.

> => *EGMLTF may provide data relating* ***to national risk assessments and more generally information on risks, threats and vulnerabilities****. The role of EGMLTF in regard of the SNRA is also to appoint national experts for the different workshops.*

European Supervisory Authorities (ESAs): the ESAs (European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority) are tasked under article 6(5) of Directive (EU) 2015/849 with the responsibility of issuing a joint opinion on the ML/TF risks **affecting the Union's financial sector**. Considering the key role the ESAs play in the identification of risks related to the financial sector, they participate directly to the discussions held within the ADHWG. In addition, regular contacts are organised between the Commission services responsible to draw up the SNRA report and the working group of the ESAs in charge of the joint opinion.

> => *ESAs may provide data relating to distinctive features of ML/TF risks from a supervisory perspective, ML risks associated with the financial sectors' systems and controls, taking into account the various typical sectorial business models, strategies and cultures*..

Other financial supervisory authorities not represented by the ESAs: considering the wide range of actors responsible for financial supervision, contacts will be held with other supervisory authorities not represented in the ESAs.

EU Financial Intelligence Units (EU FIUs): FIUs cooperate at the EU level through a group called the FIU Platform which main task is to facilitate cooperation among EU FIUs. Work of the FIU Platform and the EGMLTF should be closely coordinated

> => *The FIU Platform may provide* ***data relating to national risk assessments, distinctive features of ML/TF risks from an FIU perspective (annual reports), aggregated data on suspicious transactions reports***..

Sectorial specific expert groups: the Commission manages a number of groups of Member States experts covering the different sectors exposed to the ML/TF risks. Those networks may provide useful information and data regarding their respective sectors.

=> Such experts group may be consulted especially for preparing the assessment of the sectors' vulnerability.

Europol: Europol is an EU agency which supports law enforcement authorities by gathering, analysing and disseminating information.

=> Europol may provide data relating to organised crime threat assessments (e.g. "organised crime threat assessment report" which includes analysis on money laundering threats). It may also provide analyses and intelligence work on AML/CFT from a law enforcement perspective.

Eurostat: Eurostat is a Directorate General of the European Commission which provides statistics at European level that enable comparisons between countries and regions.

=> Eurostat may provide data relating to series of indicators for the different stages of the AML chain, from the filing of a suspicious transaction report through to conviction (ML report 2013). It may also provide statistical data on economy, sectors and products.

Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRB): FATF is an inter-governmental body which sets standards and promotes effective implementation of legal, regulatory and operational measures for combating ML, TF and other related threats to the integrity of the international financial system. FSRBs have been established for the purpose of disseminating FATF Recommendations throughout the world. The main task of the FSRBs is to devise systems for combating ML/TF risks in their respective regions.

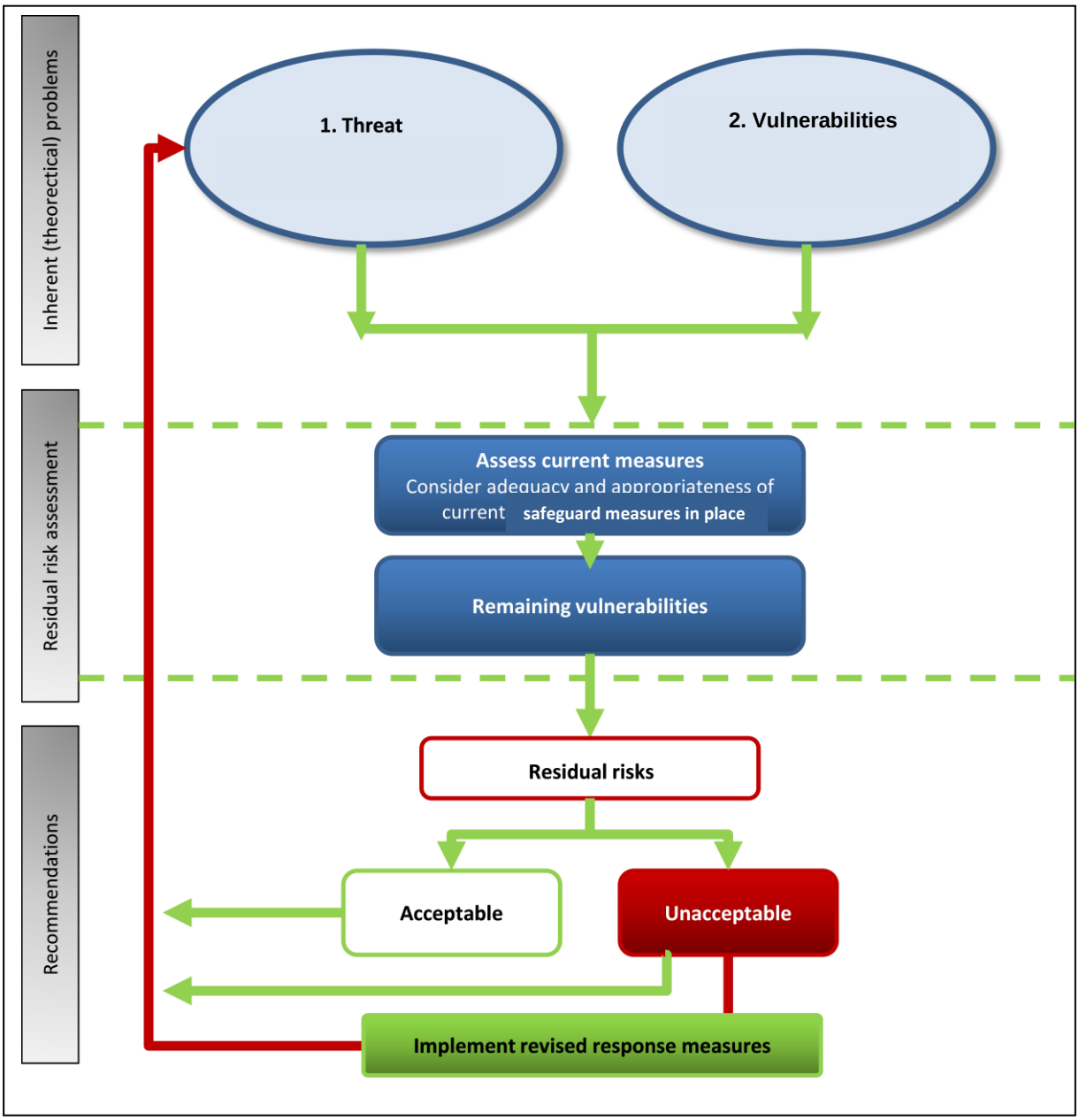
=> The FATF and FSRBs conduct evaluations of the AML/CFT systems of the Member States and are developing studies of typologies – the most common schemes used by criminals for ML/TF-that will provide useful information to feed the SNRA.

Other relevant stakeholders such as Non-Governmental Organisations (NGOs), private sector representative bodies at European level (DNBPs, financial sectors etc.) and other public or private sector organisations may also provide useful information.

4. METHODOLOGICAL APPROACH

4.1 RISK MANAGEMENT FRAMWORK

The conceptual framework for this methodology can be summarised as follows:



4.1.1 METHODOLOGICAL APPROACH

Because of their specific features, FT and ML risks will be considered and assessed within two separate work streams.

The proposed methodology is based on the following consecutive actions:

1. The identification of ML and TF mechanisms (*modi operandi*) that could constitute ML/TF risks at EU level. There are intended as ML/TF mechanisms going beyond the specificities of national jurisdictions, whatever they arise in one or several Member States and which may represent a risk from an internal market perspective.

2. An assessment of the level and nature of threats related to estimated intent and capability to exploit mechanisms for ML and TF, i.e. a clear *modi operandi* approach by "sector" (scenario based approach), in all sectors mentioned in article 2 and 4 of the Directive (EU) 2015/849. In this specific application, the assessment focuses on the estimated intent and capability of criminals to exploit existing or innovative mechanisms for ML and TF. The assessment will be based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available intelligence, information (qualitative and quantitative inputs) and in light of the agreed approach to threat assessment (clearing house threat assessment reconciliation method). The Commission, which will have a decisional power to validate the outcomes of the SNRA discussions, will assess the strategic level of threat to be respectively:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

3. An assessment of the level and nature of vulnerabilities by sector to ML/TF exploitable mechanisms (*modi operandi*). The vulnerability assessment will focus on the assessment of existing safeguards in place. Based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available information (qualitative and quantitative inputs) and in light of the agreed approach to vulnerability assessment (clearing house vulnerability

assessment reconciliation method), the Commission, which will have a decisional power to validate the outcomes of the SNRA discussions, will assess the strategic level of vulnerability to be respectively:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

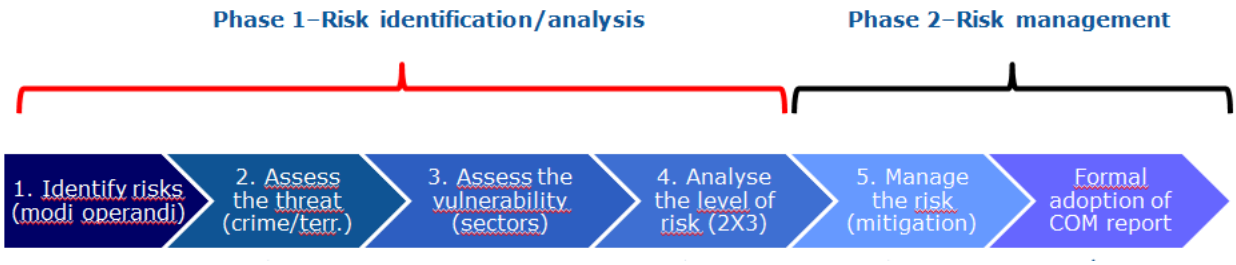
4) Very significant (value: 4)

4. Determination of the residual risk on the basis of interplay of estimated threats and vulnerabilities for each type of modus operandi. The risk assessment will be built on a risk based assessment by sector. For each sector considered a set of pre-defined *modi operandi* (ML/TF exploitable mechanisms) will be assessed in terms of risk as combination of the identified level of threat and vulnerability.

For the purpose of this risk assessment the "impact/consequences" component is regarded as constantly significant and will therefore not be assessed. The proposed methodology consequently only looks at the threats and vulnerability components. While it is important to understand the consequences associated with the ML/TF activities (physical, social, environmental, economic and structural consequences), from a methodological point of view it is particularly challenging to measure their consequences in quantifiable or numerical terms. **For the purpose of this risk assessment it is therefore assumed that ML/TF activities generate constant significant negative effects** on the transparency, good governance and the accountability of public and private EU institutions, cause significant damage to EU countries national security and have both direct and indirect impact on the EU economy. From a methodological point of view, as the impact/consequences component is assumed as a fix high value for the specific purpose of this risk assessment, the determination of the residual risk for each scenario (modus operandi versus scenario) will be determined by the combination of the identified level of threat and vulnerability.

5. PROCESS DESCRIPTION

The process can be summarised by the following steps:



A detailed roadmap is provided for the risk identification/analysis phase in Annex 1. This roadmap foresees the following consecutive actions:

5.1. STEP 1: RISK IDENTIFICATION

The first step consists in identifying the exact scope in terms of ML/TF risks to be assessed at a later stage of the risk assessment process. For the specific purpose of the SNRA as defined in Directive (EU) 2015/849, risks identification should be intended as defining a list of **known or suspected** ML/TF threats along with the related sectors exploited by criminals to successfully perpetrate ML and/or TF activities. The risk of ML and TF is not the same in every case. Accordingly, a holistic risk-based approach should be used. While the risks identification process will rely largely on known threats, it is important to give due consideration to innovative or emerging threats for which it is reasonable to assume a lack of consolidated safeguards in place. At this stage, the objective is to identify the nature of the risks scenarios (*threats versus exploitable sectors*) and those which are the most relevant considering the scope of the risk assessment. It does not seek to assess the level of these risks (significant or non-significant) which will be the objective at a later stage (estimated level of threats and vulnerabilities determining the residual risk).

5.2. STEP 2: THREAT component

This second step consists in assessing the level of threat (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the *scenario* (ML and TF

processes *versus* exploitable sector) identified in step 1[24]. The assessment will be based on the estimated combined assessment of intent and capability of criminals to change or transfer illegitimate or legitimate funds. The assessment of the threat level for each identified risk should lead to a threat assessment level common to the EU as a whole. At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method.

The Commission will validate the outcomes of the threat assessment clearing house reconciliation method[25].

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat[26]) successful or foiled, and the perceived attractiveness of ML/TF through a specific mechanism. While the broad intent to ML/TF is assessed as being constantly high, intent to use specific modus operandi differs depending of the attractiveness of the ML/TF modus operandi, and the known existence of AML/CFT safeguards.

The risk assessment will therefore consider, on a scenario by scenario basis, the level of intent to exploit (IT) ML/TF mechanisms.

The "capability" component of the threat is understood as the capability of criminals to successfully change or transfer the ML proceeds of crime and to successfully transfer illegitimate or legitimate funds to financially maintaining a terrorist network.

The assessment of the capability component will consider the ease of using a specific ML/TF modus operandi for (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

[24] Both the threat and vulnerability assessment are built around a four scale rating. Different rating can be considered but this latter presents the advantage (compared to a three or two scale rating) to capture better qualitative differences between the different risks. The resulting risk level is also based on a four scale rating.

[25] The clearing house reconciliation method has proven its efficacy in the framework of several EU risk assessments in the field of aviation security. For those risk assessments requiring a common EU position, which is the case for the supranational FT/ML risk assessment, the clearing house reconciliation method has proved its efficacy in providing the necessary working arrangements facilitating the achievement of a common position.

[26] It measures the concrete occurrence of the threat on the territory. The data used originate from the evidence available on the subject of reports to the particular offence or class of offences.

5.3. STEP 3: VULNERABILITY

This third step consists in assessing the level of vulnerability (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the scenario (ML and TF processes versus exploitable sector) identified in step 1.

For each of the scenario identified in step 1, the vulnerability assessment **will focus on the existence and effectiveness of safeguards in place**. The more effective safeguards in place, the lower vulnerabilities and risk are.

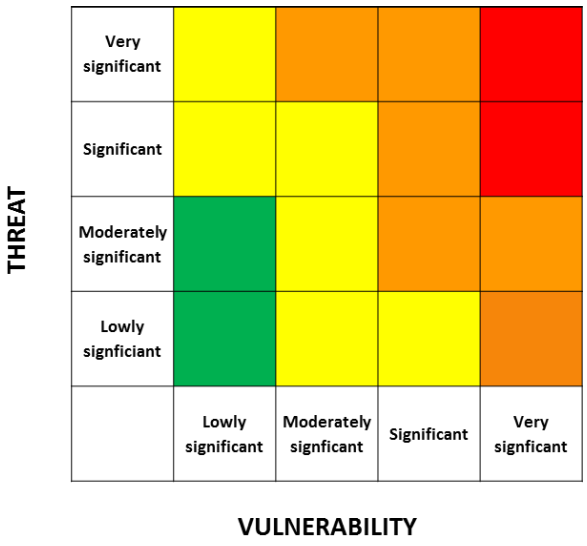
The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in step 1, required to implement the AML/CFT legislation.

For the specific purpose and scope of the SNRA, the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the EU wide nature of the ML/TF risks to be considered in the SNRA, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other AML authorities and international cooperation, including between AML supervisors.

The assessment of ML/TF vulnerabilities of the system as a whole will be based on the data collected and analysed by relevant supervisory authorities, the FIU and national authorities.

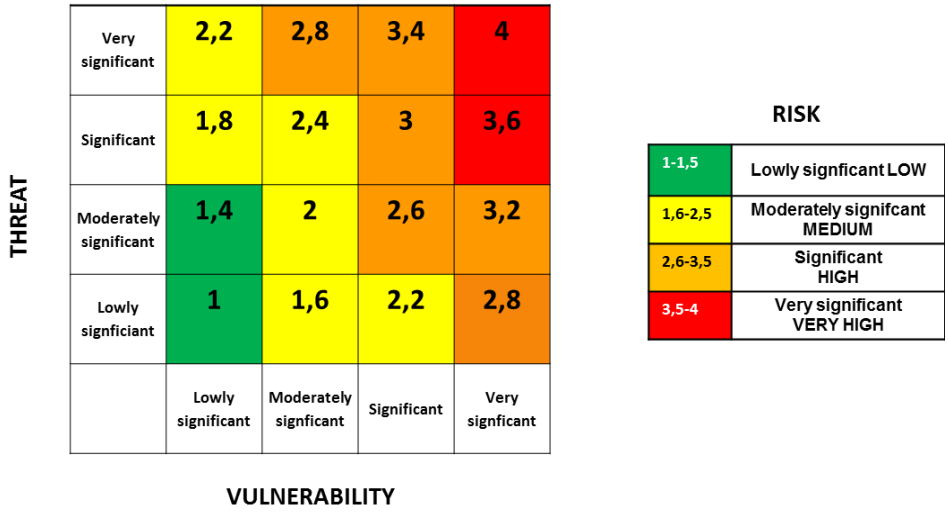
5.4. STEP 4: RESIDUAL RISK

The outcomes of steps 2A/B (threat assessment) and 3A/B (vulnerability assessment) will determine the risk level for each identified risk (steps 1A/B), as combination (matrix approach) of the assessed threat and vulnerability level.



The risk level is ultimately determined by combination between the threat *versus* vulnerability. The risk matrix determining this risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) - assuming that the vulnerability component has more capacity in

determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given modus operandi – thus impacting ultimately the level of threat.



6. INVOLVEMENT OF PRIVATE SECTOR AND CIVIL SOCIETY

The Commission will consult the private sector and civil society during the process. It will organise dedicated workshops with the four main groups of private sector stakeholders (financial sector, legal professions, other obliged entities, Non-Governmental Organisations). The Commission will organise those workshops at two steps in the process:

- Following the risk identification: consultation on the basis of already identified risks and collection of feedback regarding the risk identification (January-February 2016)

- Following the finalization of the risk assessment: consultation on the outcome and possible mitigating actions (November 2016)

7. REASSESSMENT/EX NOVO ASSESSMENT

Based on available intelligence and information, the Commission will propose further rounds of the risk assessment to reassess the evolving threat situation or new emerging threats. The

Commission ensures an updating of the risk assessment every two years, or more frequently if appropriate.

Unless there are exceptional circumstances, the first update of the SNRA would take place 2 years after the issuing of the initial SNRA report (i.e. by June 2019). This first update will be drawn up through a lighter procedure. Such lighter procedure will imply the gathering of information by written procedure (e.g. questionnaire) and will focus on the implementation of the Commission recommendations concerning the mitigating measures, and the evaluation of the risks following the mitigation.

The Commission will then assess the experience gained and, if need be, adapt its methodological approach. The second update (by 2021) would likely follow the full standard methodology for a more comprehensive assessment. It will consist of assessing the relevance of the first risk assessment outcomes by including new emerging risks.

Annex 1

Road map

Annex 1 Road Map

STEP 1/A: November 2015 – dedicated meeting: TF risks identification

Location: DG HOME secure zone

COMPOSITION: Member States experts (to be appointed by MS authorities)[27], FIU, COM (DG JUST, DG HOME), Europol, EU Intcen, ESAs

OBJECTIVE: the meeting should lead to identify TF risks (methods/modi operandi) to be considered within the risk assessment exercise according to the scope of the SNRA.

SOURCES (non-exhaustive): open sources, inputs from national risk assessment, classified threat assessment on TF issued by EU Intcen (including an update available by September 2015), inputs from Europol, TF offences listed by FAFT, intelligence from FIU.

METHODOLOGY: based on the sources above, COM will facilitate a discussion paper listing potential TF risks to be considered within the risk assessment and to be assessed a later stage (threat and vulnerability assessment). The expert group will be requested to consider their relevance in the framework of the SNRA scope and to assess whether other risks should be included.

END RESULT: define a list of TF risks (modi operandi/methods for TF) to be considered within the risk assessment.

STEP 1/B: November 2015 – dedicated meeting: ML risks identification

Location: standard meeting room

COMPOSITION: Member States experts (to be appointed by MS authorities)28, COM (DG JUST, DG HOME), Europol, ESAs.

[27] As far as the MS experts are concerned, their appointment is left to the appreciation of Member States by considering the specific expertise required for each dedicated phase of the risk assessment. For sake of efficiency, it should be ensured that the MS experts represented in the experts meetings are able to bring a position and to provide elements that has been defined and agreed at national level following a coordination process.

OBJECTIVE: the meeting should lead to identify ML risks (methods/modi operandi) to be considered within the risk assessment exercise according to the scope of the SNRA.

SOURCES (non-exhaustive)**:** open sources, inputs from national risk assessment, available threat assessment on ML, inputs from Europol, ML offences listed by FAFT, intelligence from FIU.

METHODOLOGY: based on the sources above, COM will facilitate a discussion paper listing potential ML risks to be considered within the risk assessment and to be assessed a later stage (threat and vulnerability assessment). The expert group will be requested to consider their relevance in the framework of the SNRA scope and to assess whether other risks should be included.

END RESULT: define a list of ML risks (modi operandi/methods for ML) to be considered within the risk assessment.

STEP 2/A: March/April 2016 – dedicated meeting: assessing the level of threat for TF risk identified in step 1/A

Location: DG HOME secure zone

COMPOSITION: Member States experts (to be appointed by MS authorities)[29], COM (DG JUST, DG HOME), Europol, EU Intcen.

OBJECTIVE: based on the outcomes of step 1/A) the meeting should lead for each TF identified risk to assess its threat level according to a four scale approach:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

[28] See footnote 3
[29] See footnote 3

4) Very significant (value: 4)

SOURCES(non-exhaustive)**:** open sources, inputs from national risk assessment, available threat assessment on financing terrorism (EU Intcen), inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sector's available statistics from judicial records.

METHODOLOGY: the assessment of the threat level for each TF identified risk as resulting from step 1/A, should led to a threat assessment level common to the EU as a whole.

At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method.

Threat assessment clearing house reconciliation method: experts will propose an estimated level of threat for each risk identified in step 1/A. Discrepancies in threat estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed.

Should a difference of estimates remain –these experts will attempt to determine whether the higher threat estimate is primarily due to an estimated higher threat in a specific field or Member State rather than all EU Member States equally. If so, the level of threat which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the threat **assessment reconciliation method**

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat) successful or foiled, and the perceived attractiveness of TF through a specific method/mechanism. While the broad intent to TF is assessed as being constantly high, intent to use specific modus operandi/methods differs depending of the attractiveness of the modus operandi and the known existence of CFT safeguards.

The "capability" component of the threat is understood as the capability of threat groups (terrorists) to successfully transfer illegitimate or legitimate funds to financially maintaining a terrorist network.

The assessment of the capability component will consider the ease of using a specific modus operandi for TF (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

Table 1: the threat component (financing terrorism risks) will be assessed according to a four scale threat level:

LOWLY SIGNIFICANT (value: 1)	No indicators that criminals have the intention to exploit this modus operandi for ML/TF. The modus operandi is extremely difficult to access and/or may cost more than other options and perceived as unattractive and/or highly insecure. No indicators that criminals have the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires sophisticated planning, knowledge and/or high technical expertise than other options. **The threat related to the use of this modus operandi is lowly significant.**
MODERATELY SIGNIFICANT (value: 2)	Criminals may have vague intentions to exploit this modus operandi for ML/TF. The modus operandi is difficult to access and/or may cost more than other options and perceived as unattractive and/or insecure. Few indicators that criminals have some of the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires planning, knowledge and/or technical expertise than other options. **The threat related to the use of this modus operandi is moderately significant.**
SIGNIFICANT (value: 3)	Criminals have exploited this modus operandi for ML/TF. The modus operandi is accessible and/or represents a financially viable option. The modus operandi is perceived as rather attractive and/or fairly secure. Criminals have the necessary capabilities to exploit this modus operandi. The modus operandi requires moderate levels of planning, knowledge and/or technical expertise. **The threat related to the use of this modus operandi is significant.**
VERY SIGNIFICANT (value: 4)	Criminals have recurrently exploited this modus operandi for ML/TF. The modus operandi is widely accessible and available via a number of means and/or relatively low cost. The modus operandi is perceived as attractive and/or secure. Criminals are known to have the necessary capabilities. The modus operandi is relatively easy to abuse, requires little planning, knowledge and/or technical expertise required compared to other options. **The threat related to the use of this modus operandi is very significant.**

END RESULT: assessing TF threat level for each identified risk according to the 4 scale approach.

STEP 2/B March/April 2016 – dedicated meeting: assessing the level of threat for each ML risk identified in step 1/B
Location: DG HOME secure zone

COMPOSITION: Member States experts (to be appointed by MS authorities)[30], COM (DG JUST, DG HOME), Europol, EU Intcen.

OBJECTIVE: based on the outcomes of step 1/B, the meeting should lead, for each ML identified risk, to assess its threat level according to a four scale threat level:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES (non-exhaustive)**:** open sources, inputs from national risk assessment, inputs from Commission services, inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sectors, available statistics from judicial records.

METHODOLOGY: the assessment of the threat level for each identified ML risk as resulting from step 1/B, should led to a threat assessment level common to the EU as a whole. While capabilities and intent may be very different in Member States, with certain risks extremely significant in some countries and less relevant in other countries, the scope of the SNRA requires to identify a threat assessment level common to the EU as a whole.

[30] See footnote 3

At this regard, it is suggested the strategic level of threat for each risk will be assessed according to the threat assessment clearing house reconciliation method.

Threat assessment clearing house reconciliation method: experts will propose an estimated level of threat for each ML risk identified in step 1/B. Discrepancies in threat estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed.

Should a difference of estimates remain – e.g. with some experts estimating threat to be "medium" and others "high" – these experts will attempt to determine whether the higher threat estimate is primarily due to an estimated higher threat in a specific field or Member State rather than all EU Member States equally. If so, the level of threat which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the threat **assessment reconciliation method**

The "Intent" component of the threat will rely on known intent (concrete occurrence of the threat) successful or foiled, and the perceived attractiveness of ML through a specific method/mechanism. Intent to use specific modus operandi/methods differs depending of the attractiveness of the modus operandi and the known existence of AML safeguards.

The "capability" component of the threat is understood as the capability of criminals to successfully laundering and transfer illegitimate funds.

The assessment of the capability component will consider the ease of using a specific modus operandi for ML (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

Table 2: the threat component (money laundering risks) will be assessed according to a four scale threat level:

LOWLY SIGNIFICANT (value: 1)	No indicators that criminals have the intention to exploit this modus operandi for ML/TF. The modus operandi is extremely difficult to access and/or may cost more than other options and perceived as unattractive and/or highly insecure. No indicators that criminals have the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires sophisticated planning, knowledge and/or high technical expertise than other options. **The threat related to the use of this modus operandi is lowly significant.**
MODERATELY SIGNIFICANT (value: 2)	Criminals may have vague intentions to exploit this modus operandi for ML/TF. The modus operandi is difficult to access and/or may cost more than other options and perceived as unattractive and/or insecure. Few indicators that criminals have some of the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires planning, knowledge and/or technical expertise than other options. **The threat related to the use of this modus operandi is moderately significant.**
SIGNIFICANT (value: 3)	Criminals have exploited this modus operandi for ML/TF. The modus operandi is accessible and/or represents a financially viable option. The modus operandi is perceived as rather attractive and/or fairly secure. Criminals have the necessary capabilities to exploit this modus operandi. The modus operandi requires moderate levels of planning, knowledge and/or technical expertise. **The threat related to the use of this modus operandi is significant.**
VERY SIGNIFICANT (value: 4)	Criminals have recurrently exploited this modus operandi for ML/TF. The modus operandi is widely accessible and available via a number of means and/or relatively low cost. The modus operandi is perceived as attractive and/or secure. Criminals are known to have the necessary capabilities. The modus operandi is relatively easy to abuse, requires little planning, knowledge and/or technical expertise required compared to other options. **The threat related to the use of this modus operandi is very significant.**

END RESULT: assessing threat level for each ML identified risk according to the four scale threat level.

STEP 3/A: May- July 2016 – dedicated meeting: assessing the level of vulnerability for each TF risk identified in step 2/A

Location: standard meeting room

COMPOSITION: Member States experts (to be appointed by MS authorities)[31], COM (DG JUST, DG HOME), Europol, ESAs.

OBJECTIVE: based on the outcomes of step 1/A, the meeting should led, for each identified TF risk, to assess its vulnerability level according to a four scale vulnerability level:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES (non-exhaustive**):** open sources, inputs from national risk assessment, available threat assessment on TF (EU Intcen), inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sectors, and available statistics from judicial records.

METHODOLOGY: the assessment of the vulnerability level for each identified TF risk as resulting from step 1/A, should led to a vulnerability assessment level common to the EU as a whole as result, among others, of differences between the regulatory frameworks of Member States which might induce vulnerabilities at a supra national level.

The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in step 1A, required to implement the TF legislation. Consideration will be also given to threats which cannot be linked to a sector.

For the specific purpose and scope of the SNRA, the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the EU wide nature of the risks to be

[31] See footnote 3

considered in the SNRA assessment, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other CFT authorities and international cooperation, including between CFT supervisors.

One of the main components of the vulnerability assessment will consider, for each category of obliged parties, the specific risk and effectiveness of CFT safeguards in place.

Table 3: the vulnerability component will be assessed according to a four scale vulnerability level:

LOWLY SIGNIFICANT (value: 1)	[Within the sector/area considered, deterrence measures and controls exist and are effective at deterring money laundering and financing terrorism. The sector shows a positive organisational framework and a negligible exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **RISK EXPOSURE** - No or very limited products, services or transactions that facilitate speedy or anonymous transactions; secured and/or monitored delivery channels; low level of financial transactions; low level of cash based transactions; high quality management of new technologies and/or new payment methods - Very limited volume of higher risk customers[32]; high ability to manage corporate entities or trusts in customer relationships - No or very limited business and customer based in areas identified as high risk[33]; low level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows a satisfactory level of awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from a positive organisational framework. - Competent authorities provide a comprehensive ML/TF risk assessment related to the sector and LEAs have a high ability to counter ML/TF risks (a range of ML/TF cases is visible and highly likely to be detected,

[32] A non-exhaustive list of factors and type of evidence of potentially higher risk customer is included in Annex 3 of Directive (EU) 2015/849

[33] A non-exhaustive list of factors and type of evidence of potentially higher risk countries is included in Annex 3 of Directive (EU) 2015/849. In the same text, Article 9 tasks the Commission to identify high-risk third countries

	leading to investigation, prosecution and convictions) - Good ability of the FIU to detect and analyse the risks, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators and a sufficient amount of resources to actually perform the risk-analysis. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework is commensurate to the risks inherent to this sector. - Controls [defined by the legislation] are effectively applied by the sector. Reliable CDD/identification mechanisms are in place to ensure adequate identification and verification process of a customer. Internal controls are applied by obliged entities in a robust manner (e.g. risk management, record keeping, training). Obliged entities are effectively reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a good level of sharing of information **=> Lowly-significant vulnerabilities.**
MODERATELY SIGNIFICANT (value: 2)	[Within the sector/area considered, deterrence measures and controls exist and are reasonably effective at deterring money laundering and financing terrorism. The sector shows an organisational framework presenting some weaknesses and/or an exposure to the risk of ML/TF.]. **Illustrative assessment criteria**: **RISK EXPOSURE** - Limited products, services and transactions that facilitate speedy or anonymous transactions; mostly secured and/or monitored delivery channels; rather significant level of financial transactions; rather significant cash based transactions; good management of new technologies and/or new payment methods - Few higher risk customers; good ability to manage corporate entities or trusts in customer relationships - Some business and customer are based in areas identified as high risk; rather significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows some awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from an organisational framework which shows some weaknesses. - Competent authorities provide a reasonable ML/TF risk assessment related to the sector and LEAs have a good ability to counter ML/TF risks (a range of ML/TF cases is visible and likely to be detected, leading to some investigations, prosecutions and convictions

	- FIU can detect and analyse the risks in certain circumstances, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework covers in major parts the risks inherent to this sector - Controls [defined by the legislation] are applied by the sector but presenting some weaknesses. Reliable CDD/identification mechanisms are in place but do not ensure systematically an adequate identification and verification process of a customer. Internal controls are applied by obliged entities to some extent (e.g. risk management, record keeping, training). Obliged entities are reporting few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a partial sharing of information. **=> moderately significant vulnerabilities**
SIGNIFICANT (value: 3)	[Within the sector/area considered, deterrence measures and controls have limited effects in deterring criminal/terrorist abuse of the service. The sector shows an organisational framework presenting very significant weaknesses and/or a significant exposure to the risk of ML/TF.]. **Illustrative assessment criteria:** **RISK EXPOSURE** - Significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; few secured and/or monitored delivery channels; significant level of financial transactions; significant cash based transactions; low management of new technologies and/or new payment methods - Significant volumes of higher risk customers; low ability to manage corporate entities or trusts in customer relationships - Major part of business and customer is based in areas identified as high risk; significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows limited awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, and training, allocated resources). The sector benefits from a limited organisational framework. - Competent authorities provide for a limited ML/TF risk assessment to the sector and LEAs have low capacity to counter ML/TF risks (only some ML/TF cases are visible and unlikely to be detected, leading to few investigations, prosecutions and convictions) - The FIU can detect and analyse the risks only in limited circumstances

	which allows only a limited functioning of gathering information through STR. **<u>LEGAL FRAMEWORK AND CONTROLS</u>** - The existing legal framework does not cover the most substantial parts of the risks inherent to this sector. - Controls applied by the sector present significant weaknesses. Few reliable CDD/identification mechanisms are in place and does not allow an effective identification and verification process of a customer. Internal controls are applied by obliged entities with very significant weaknesses (e.g. risk management, record keeping, training). Obliged entities are reporting very few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows on few possibilities of sharing of information => **Significant vulnerabilities**
VERY SIGNIFICANT (value: 4)	[Within the sector/area considered, there are extremely limited or no measures and controls in place, or they are not working as intended. The sector shows an organisational framework presenting highly significant weakness and/or a high exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **<u>RISK EXPOSURE</u>** - Very significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; no secured and/or monitored delivery channels; very significant level of financial transactions; very significant cash based transactions; no management of new technologies and/or new payment methods - Very significant volumes of higher risk customers[34]; no ability to manage corporate entities or trusts in customer relationships - Business and customer are based in areas identified as high risk[35]; very significant level of cross-border movements of funds; **<u>AWARNESS OF THE RISK VULNERABILITY</u>** - Sector concerned shows no awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector has no adequate organisational framework to address the ML/TF risks.

[34] A non-exhaustive list of factors and type of evidence of potentially higher risk customer is included in Annex 3 of Directive (EU) 2015/849

[35] A non-exhaustive list of factors and type of evidence of potentially higher risk countries is included in Annex 3 of Directive (EU) 2015/849. In the same text, Article 9 tasks the Commission to identify high-risk third countries

	- Competent authorities don't provide for any ML/TF risks assessment to the sector and LEAs have no ability to counter ML/TF risks (detection is very difficult and there are very few/no financial or other indicators of suspicious activity. The level of investigations, prosecutions and confiscations is extremely low) - The FIU can detect the risks in very limited circumstances or in no circumstances. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the risks inherent to this sector - Controls applied by the sector present very significant weaknesses. No reliable CDD/identification mechanisms are in place and the basic identification and verification requirement process of a customer is not fulfilled. Internal controls are not properly applied by obliged entities (e.g. risk management, record keeping, training). Obliged entities are not reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, does not exist or does not allow sharing of information **=> very significant vulnerabilities**

WORKING ARRANGEMENTS

It is suggested the strategic level of vulnerability for each TF risk will be assessed according to the vulnerability assessment clearing house reconciliation method.

Experts will propose an estimated level of vulnerability for each TF risk identified in step 1/A. Discrepancies in vulnerability estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed. Should a difference of estimates remain these experts will attempt to determine whether the higher vulnerability estimate is primarily due to an estimated higher vulnerability in a specific field or Member State rather than all EU Member States equally. If so, the level of vulnerability which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the vulnerability **assessment reconciliation method**

STEP 3/B: May-July 2016 – dedicated meeting: assessing the level of vulnerability for each ML risk identified in step 1/B

Location: standard meeting room

COMPOSITION: Member States experts (to be appointed by MS authorities)[36], COM (DG JUST, DG HOME), Europol, ESAs.

OBJECTIVE: based on the outcomes of step 1/B, the meeting should led, for each identified ML risk, to assess its vulnerability level according to a four scale vulnerability level:

1) Lowly significant (value: 1)

2) Moderately significant (value: 2)

3) Significant (value: 3)

4) Very significant (value: 4)

SOURCES (non-exhaustive)**:** open sources, inputs from national risk assessment, inputs from Commission services, inputs from Europol, available intelligence from Member States / FIU, inputs from financial sectors supervisors, non-financial sectors supervisors, private sectors, and available statistics from judicial records.

METHODOLOGY: the assessment of the vulnerability level for each identified ML risk as resulting from step 1/B, should led to a vulnerability assessment level common to the EU as a whole as result, among others, of differences between the regulatory frameworks of Member States which might induce vulnerabilities at a supra national level.

The vulnerability assessment will be performed for the areas/sectors, related to the modus operandi identified in step 1B, required to implement the ML legislation. Consideration will be also given to threats which cannot be linked to a sector.

For the specific purpose and scope of the SNRA the vulnerability assessment will consider primarily the existence of national, EU and international legislation and their effective

[36] See footnote 3

implementation at national level. By taking into account the EU wide nature of the risks to be considered in the SNRA, particular attention should also be paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other AML authorities and international cooperation, including between AML supervisors.

One of the main components of the vulnerability assessment will consider, for each category of sectors, the specific risk and effectiveness of AML safeguards in place.

Table 4: **The vulnerability component will be assessed according to a four scale vulnerability level:**

LOWLY SIGNIFICANT (value: 1)	[Within the sector/area considered, deterrence measures and controls exist and are effective at deterring money laundering and financing terrorism. The sector shows a positive organisational framework and a negligible exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **RISK EXPOSURE** - No or very limited products, services or transactions that facilitate speedy or anonymous transactions; secured and/or monitored delivery channels; low level of financial transactions; low level of cash based transactions; high quality management of new technologies and/or new payment methods - Very limited volume of higher risk customers; high ability to manage corporate entities or trusts in customer relationships - No or very limited business and customer based in areas identified as high risk; low level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows a satisfactory level of awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from a positive organisational framework. - Competent authorities provide a comprehensive ML/TF risk assessment related to the sector and LEAs have a high ability to counter ML/TF risks (a range of ML/TF cases is visible and highly likely to be detected, leading to investigation, prosecution and convictions) - Good ability of the FIU to detect and analyse the risks, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators and a sufficient amount of resources to

	actually perform the risk-analysis. **<u>LEGAL FRAMEWORK AND CONTROLS</u>** - The existing legal framework is commensurate to the risks inherent to this sector. - Controls [defined by the legislation] are effectively applied by the sector. Reliable CDD/identification mechanisms are in place to ensure adequate identification and verification process of a customer. Internal controls are applied by obliged entities in a robust manner (e.g. risk management, record keeping, training). Obliged entities are effectively reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a good level of sharing of information **=> Lowly-significant vulnerabilities.**
MODERATELY SIGNIFICANT (value: 2)	[Within the sector/area considered, deterrence measures and controls exist and are reasonably effective at deterring money laundering and financing terrorism. The sector shows an organisational framework presenting some weaknesses and/or an exposure to the risk of ML/TF.]. **<u>Illustrative assessment criteria</u>**: **<u>RISK EXPOSURE</u>** - Limited products, services and transactions that facilitate speedy or anonymous transactions; mostly secured and/or monitored delivery channels; rather significant level of financial transactions; rather significant cash based transactions; good management of new technologies and/or new payment methods - Few higher risk customers; good ability to manage corporate entities or trusts in customer relationships - Some business and customer are based in areas identified as high risk; rather significant level of cross-border movements of funds; **<u>AWARNESS OF THE RISK VULNERABILITY</u>** - Sector concerned shows some awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector benefits from an organisational framework which shows some weaknesses. - Competent authorities provide a reasonable ML/TF risk assessment related to the sector and LEAs have a good ability to counter ML/TF risks (a range of ML/TF cases is visible and likely to be detected, leading

	to some investigations, prosecutions and convictions - FIU can detect and analyse the risks in certain circumstances, to ensure a good functioning of gathering information through STR, in particular through the use of tailor-made indicators **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework covers in major parts the risks inherent to this sector - Controls [defined by the legislation] are applied by the sector but presenting some weaknesses. Reliable CDD/identification mechanisms are in place but do not ensure systematically an adequate identification and verification process of a customer. Internal controls are applied by obliged entities to some extent (e.g. risk management, record keeping, training). Obliged entities are reporting few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a partial sharing of information. => **moderately significant vulnerabilities**
SIGNIFICANT (value: 3)	[Within the sector/area considered, deterrence measures and controls have limited effects in deterring criminal/terrorist abuse of the service. The sector shows an organisational framework presenting very significant weaknesses and/or a significant exposure to the risk of ML/TF.]. **Illustrative assessment criteria:** **RISK EXPOSURE** - Significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; few secured and/or monitored delivery channels; significant level of financial transactions; significant cash based transactions; low management of new technologies and/or new payment methods - Significant volumes of higher risk customers; low ability to manage corporate entities or trusts in customer relationships - Major part of business and customer is based in areas identified as high risk; significant level of cross-border movements of funds; **AWARNESS OF THE RISK VULNERABILITY** - Sector concerned shows limited awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, and training, allocated resources). The sector benefits from a limited organisational framework. - Competent authorities provide for a limited ML/TF risk assessment to

	the sector and LEAs have low capacity to counter ML/TF risks (only some ML/TF cases are visible and unlikely to be detected, leading to few investigations, prosecutions and convictions) - The FIU can detect and analyse the risks only in limited circumstances which allows only a limited functioning of gathering information through STR. **<u>LEGAL FRAMEWORK AND CONTROLS</u>** - The existing legal framework does not cover the most substantial parts of the risks inherent to this sector. - Controls applied by the sector present significant weaknesses. Few reliable CDD/identification mechanisms are in place and does not allow an effective identification and verification process of a customer. Internal controls are applied by obliged entities with very significant weaknesses (e.g. risk management, record keeping, training). Obliged entities are reporting very few suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows on few possibilities of sharing of information => **Significant vulnerabilities**
VERY SIGNIFICANT (value: 4)	[Within the sector/area considered, there are extremely limited or no measures and controls in place, or they are not working as intended. The sector shows an organisational framework presenting highly significant weakness and/or a high exposure to the risk of ML/TF]. **Illustrative assessment criteria:** **<u>RISK EXPOSURE</u>** - Very significant volumes of products, services and transactions that facilitate speedy or anonymous transactions; no secured and/or monitored delivery channels; very significant level of financial transactions; very significant cash based transactions; no management of new technologies and/or new payment methods - Very significant volumes of higher risk customers; no ability to manage corporate entities or trusts in customer relationships - Business and customer are based in areas identified as high risk; very significant level of cross-border movements of funds; **<u>AWARNESS OF THE RISK VULNERABILITY</u>** - Sector concerned shows no awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). The sector has no adequate organisational framework to address the

	ML/TF risks. - Competent authorities don't provide for any ML/TF risks assessment to the sector and LEAs have no ability to counter ML/TF risks (detection is very difficult and there are very few/no financial or other indicators of suspicious activity. The level of investigations, prosecutions and confiscations is extremely low) - The FIU can detect the risks in very limited circumstances or in no circumstances. **LEGAL FRAMEWORK AND CONTROLS** - The existing legal framework does not cover the risks inherent to this sector - Controls applied by the sector present very significant weaknesses. No reliable CDD/identification mechanisms are in place and the basic identification and verification requirement process of a customer is not fulfilled. Internal controls are not properly applied by obliged entities (e.g. risk management, record keeping, training). Obliged entities are not reporting suspicious transactions to FIUs. - Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, does not exist or does not allow sharing of information **=> very significant vulnerabilities**

WORKING ARRANGEMENTS

It is suggested the strategic level of vulnerability for each ML risk will be assessed according to the vulnerability assessment clearing house reconciliation method.

Experts will propose an estimated level of vulnerability for each ML risk identified in step 1/B. Discrepancies in vulnerability estimates will then be discussed multilateral (or bilaterally if needed), until the Commission considers that a common position, deemed as common to the EU as a whole, is agreed. Should a difference of estimates remain these experts will attempt to determine whether the higher vulnerability estimate is primarily due to an estimated higher vulnerability in a specific field or Member State rather than all EU Member States equally. If so, the level of vulnerability which will be retained by the Commission for the purpose of the current methodology will be that which it considers as common to the EU as a whole.

The Commission will have a decisional power to validate the outcomes of the vulnerability **assessment reconciliation method.**

STEP 4 (October 2016): Residual risk

The outcomes of steps 2A/B (threat assessment) and 3A/B (vulnerability assessment) will determine the risk level for each identified risk (steps 1A/B), as combination (matrix approach) of the assessed threat and vulnerability level.

The risk level is ultimately determined by combination between the threat *versus* vulnerability. The risk matrix determining this risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) - assuming that the vulnerability component has more capacity in determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given modus operandi – thus impacting ultimately the level of threat.

SUGGESTED ROAD MAP (summary)

- **November -December 2015:** risks' identification (financing terrorism)
- **November -December 2015:** risks' identification (money laundering)
- **January-February 2016: Private sector/civil society consultation No 1**
- **March-April 2016:** threat assessment (financing terrorism)
- **March-April 2016:** threat assessment (money laundering)
- **May-September 2016:** vulnerability assessment (financing terrorism)
- **May-September 2016:** vulnerability assessment (money laundering)
- **October 2016: consolidated overview of risks**
- **November 2016: Private sector/civil society consultation No 2**
- **March 2017: Private sector/civil society consultation No 3**
- The road map should also take into account the joint opinion provided by the European Supervisory Authorities on the financial sector to be issued by 26 December 2016

Annex 2

Risk evaluation process

ANNEX 2: Risk evaluation process

The "evaluation" of the identified and assessed risks (outcomes of the risk assessment) is out of the scope of these methodological guidelines. It shall be considered within the framework of the overall risk management process leading to the identification of mitigation measures to fill the identified residual risks. This annex is provided for information purposes only in order to present the output and the procedural steps of the risk evaluation phase.

1. Deliverables

Based on the risk analysis, the Commission will issue a risk assessment report which will consist of:

- A Commission communication including the mitigating measures (max 15 pages).

- A staff working document would complete the "political" input for a more comprehensive presentation of the risk analysis.

- If need be, a classified technical annex may be prepared to protect sensitive information (EU RESTRICTED)

2. Procedural steps

Following the delivery of the risk analysis, the Commission will carry out the following procedural steps (tentative timing only):

- Analyse the results and identify mitigating actions (by end of November 2016)

- Draft the SNRA report (by January 2017)

- Consult EGMLTF and FIU platform about the draft report (by March 2017)

- Formally adopt the SNRA report (by end of June 2017).

Annex 3

Relevant provisions of Directive 2015/849

ANNEX 3: Relevant provisions of Directive 2015/849

Article 2

(…)

2. With the exception of casinos, and following an appropriate risk assessment, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing this Directive on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

Among the factors considered in their risk assessments, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

In their risk assessments, Member States shall indicate how they have taken into account any relevant findings in the reports issued by the Commission pursuant to Article 6. (…)

Article 6

1. The Commission shall conduct an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.

To that end, the Commission shall, by 26 June 2017, draw up a report identifying, analysing and evaluating those risks at Union level. Thereafter, the Commission shall update its report every two years, or more frequently if appropriate.

2. The report referred to in paragraph 1 shall cover at least the following:

(a) the areas of the internal market that are at greatest risk;

(b) the risks associated with each relevant sector;

(c) the most widespread means used by criminals by which to launder illicit proceeds.

3. The Commission shall make the report referred to in paragraph 1 available to the Member States and obliged entities in order to assist them to identify, understand, manage and mitigate the risk of money laundering and terrorist financing, and to allow other stakeholders, including national legislators, the European Parliament, the ESAs, and representatives from FIUs to better understand the risks.

4. The Commission shall make recommendations to Member States on the measures suitable for addressing the identified risks. In the event that Member States decide not to apply any of the recommendations in their national AML/CFT regimes, they shall notify the Commission thereof and provide a justification for such a decision.

5. By 26 December 2016, the ESAs, through the Joint Committee, shall issue an opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector (the 'joint opinion'). Thereafter, the ESAs, through the Joint Committee, shall issue an opinion every two years.

6. In conducting the assessment referred to in paragraph 1, the Commission shall organise the work at Union level, shall take into account the joint opinions referred to in paragraph 5 and shall involve the Member States' experts in the area of AML/CFT, representatives from FIUs and other Union level bodies where appropriate. The Commission shall make the joint opinions available to the Member States and obliged entities in order to assist them to identify, manage and mitigate the risk of money laundering and terrorist financing.

7. Every two years, or more frequently if appropriate, the Commission shall submit a report to the European Parliament and to the Council on the findings resulting from the regular risk assessments and the action taken based on those findings. (…)

Article 7

1. Each Member State shall take appropriate steps to identify, assess, understand and mitigate the risks of money laundering and terrorist financing affecting it, as well as any data protection concerns in that regard. It shall keep that risk assessment up to date.

2. Each Member State shall designate an authority or establish a mechanism by which to coordinate the national response to the risks referred to in paragraph 1. The identity of that authority or the description of the mechanism shall be notified to the Commission, the ESAs, and other Member States.

3. In carrying out the risk assessments referred to in paragraph 1 of this Article, Member States shall make use of the findings of the report referred to in Article 6(1).

Article 9

Third-country policy

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.

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):

(1) Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;

(b) customers that are resident in geographical areas of higher risk as set out in point (3);

(c) legal persons or arrangements that are personal asset-holding vehicles;

(d) companies that have nominee shareholders or shares in bearer form;

(e) businesses that are cash-intensive;

(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

(2) Product, service, transaction or delivery channel risk factors:

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(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.

Annex 4

Terminology

ANNEX 4: terminology

Acceptable risk means the level of risk that is acceptable after mitigating the risk. Considering that it is virtually impossible to reduse AML/CTF risk to zero, some ML/TF risks will always remain.

Capability means the (extent of someone's) power or ability to exploit mechanism/process for ML/TF.

Consequence means the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector. As stated above, ideally a risk assessment involves making judgments about threats, vulnerabilities and consequences. Given the challenges in determining or estimating the consequences of ML and TF it is accepted that incorporating consequence into risk assessments may not involve particularly sophisticated approaches, and that countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. The key is that the risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts.

Evaluation refers to the last stage of risk assessment. It involves taking the results found during the analysis process to determine priorities for addressing the risks, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for their mitigation.

Intent means the aim or purpose to exploit a mechanism/process for ML/TF.

Internal market comprises an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured (article 26 TFEU).

Money Laundering means the following conduct, when committed intentionally:

(a) 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 such an activity to evade the legal consequences of that person's action;

(b) 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;

(c) 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;

(d) participation in, association with, attempts to commit and aiding, abetting, facilitating and counselling any of the activities referred to in points (a), (b) and (c).

Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Money laundering and terrorist financing risk assessment means a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand ML/TF risks and serves as a first step in addressing them. Ideally, a risk assessment, involves making judgments about threats, vulnerabilities and consequences.

Residual risk means the inherent risk minus mitigating controls. The residual risk represents the risk remaining after the consideration of controls in place.

Risk means the ability of a threat to exploit vulnerability

Sector means a group of professions and categories of undertakings (financial or non-financial) that may be misused for the purpose of money laundering and terrorist financing. This definition covers at least the following entities:

(1) credit institutions;

(2) financial institutions;

(3) the following natural or legal persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or immovable property transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:

(i) buying and selling of immovable property or business entities;

(ii) managing of client money, securities or other assets;

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies, foundations, or similar legal arrangements;

(c) trust or company service providers other than those referred to in points (a) or (b);

(d) estate agents;

(e) other natural or legal persons trading in goods, to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(f) providers of gambling services.

Other professions and categories of undertakings which are covered at national level or which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes may also be covered by this definition.

Supranational risk means a risk of ML and TF affecting the *internal market* which presents common characteristics that could arise in several or in one Member State only and/or that could also have external causes.

Terrorist Financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they 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.

Threat means a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. *Threat* is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment. In some

instances, certain types of threat assessments might serve as a precursor for a ML/TF risk assessment.

Vulnerabilities means those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at *vulnerabilities* as distinct from *threat* means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.

Annex 5

Tables of acronymes

ANNEX 5: Table of Acronymes

ML	Money laundering
TF	Terrorist financing
AML/CFT	Anti-money laundering and countering terrorist financing
SNRA	Supranational risk assessment
ESAs	European supervisory authorities
ADHWG	Ad Hoc Working Group
LEA	Law Enforcement Authorities
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit

ANNEX 4 - OVERVIEW OF ENTITIES SUBJECT TO THE AML/CFT FRAMEWORK

OVERVIEW OF ENTITIES SUBJECT TO THE AML/CFT FRAMEWORK

The list of obliged entities subject to the AML/CFT framework is defined in article 2 of Directive 2005/60. It comprises credit institutions, financial institutions, and the following legal or natural persons acting in the exercise of their professional activities: auditors, external accountants, tax advisors, notaries and other independent legal professionals, trust and company services providers, real estate agents and dealers in high value goods accepting payments in cash beyond EUR 15 000.

In term of number of obliged entities, the following overview gives an estimate of the size of those sectors in the EU based on data collected on 22 out of 28 Member States:

Number of obliged entities per Member States (2015)

	AUSTRIA	BELGIUM	BULGARIA	CZECH REPUBLIC	CYPRUS	DENMARK	ESTONIA	FINLAND	FRANCE	GERMANY	GREECE	HUNGARY	ITALY	IRELAND	LATVIA	MALTA	NETHERLAND	POLAND	PORTUGAL	SPAIN	SLOVAKIA	SLOVENIA	Total
Financial sector																							(indicative)
Payment institutions*, excluding currency exchange offices (bureaux de change)	4	24	10	18	9	11	12	311	51	32	10	8	n/a	33	37	26	37	36	16	61	10	4	760
Currency exchange offices (bureau de	3	14	738	984	4	67	n/a	16	180	12	10	268	n/a	16	50	8	8	5.022	7	2.617	1.146	24	11.194
Credit institutions*, including branches	909	92	28	57	56	75	9	2.549	451	1.740	38	142	n/a	51	26	28	175	653	162	219	27	23	7.510
E-money institutions*, excluding currency exchange offices (bureaux de change)	0	9	2	2	7	4	0	44	18	6	1	1	n/a	2	15	10	1	0	1	5	2	1	131
Other financial institutions*	n/a	31	30	n/a	n/a	65	2	140	134	1.300	18	254	n/a	492	n/a	10	n/a	225	150	65	104.655	n/a	107.571
Insurance undertakings*	27	45	46	20	10	17	4	69	265	84	22	19	56	58	2	9	280	27	21	114	16	11	1.222
Investment firms*	123	50	70	34	185	39	3	119	131	138	114	20	n/a	138	4	61	250	64	33	277	34	5	1.892
Collective investments undertakings marketing their units or shares	n/a	1	111	56	13	97	17	0	627	n/a	16	67	n/a	2.581	17	271	319	815	n/a	300	0	9	5.317
Insurance intermediaries*	17.181	8.882	398	147.381	20	164	39	0	22.818	n/a	1500	446	40.779	1.981	63	45	3.875	49.126	12.079	2.739	0	11.428	320.944
Other financial sector's obliged entities when designated by Member States at national	n/a	1	9	12	n/a	109	n/a	n/a	5.222	n/a		101	n/a	n/a	41	46	332	49	11	138	n/a	n/a	6.071
Non-financial sector																							
Lawyers	6.138	16.344	1.466	16.244	3.181	6.205	934	2.840	40.000	163.513	42.001	12.601	n/a	n/a	1.363	287	5.100	15.949	n/a	853	5.942	1.684	342.645
Notaries	500	1.172	807	449	n/a	n/a	95	0	10.278	7.156	3.500	316	4.819	n/a	108	277	3.125	3.326	n/a	2.927	344	93	39.292
External accountants/ auditors	2.281	11.466	796	2.263	654	5.000	n/a	6.446	28.150	21.416	45 audit firms 1.210 auditors 1.351 legal entities & 15.000 natural persons	58.657	116.245	n/a	8.288	416	8.747	<40000	1.378	7 157	129.053	4.817	422.424
Tax advisors			9.858	4.658		N/A	n/a	4.837	n/a	82.382		9.784	n/a	n/a	3.185	137	24.300	7.120	n/a		931	3.000	150.192
Real-estate agents	4.792	8.800	2.469	14.237	271	3.295	n/a	1.600	20.000	19.000	4.000	2.058	n/a	n/a	2.170	102	9.000	4.083	50.963	5.559	58.485	223	211.107
Traders in goods receiving cash payments above 10 000 Euros	5.110	n/a	n/a	n/a	n/a	n/a	n/a	50.000	n/a	no information available currently	data not available	408	n/a	n/a	542	Not Available	41.000	n/a	36.100	Cash payments above 2 500 Euros are forbidden by Law 7/2012	0	n/a	133.160
Trust or company service providers	16.912	n/a	n/a	792	3.602	480	79	0	n/a	n/a		n/a	n/a	n/a		688	500	n/a	n/a	68	22.997	n/a	46.118
Casinos	1	9	25	34		33	14	1	200	19		8	n/a	n/a	14	5	1	49	n/a	42	4	37	496
Providers of gambling services (excluding casinos)	n/a	n/a	822	27	11	n/a	n/a	2.824	tbc	9189 (regulated) and 5098 online provider	12 landbased & 24 online gambling providers	10	n/a	n/a	14	Not considered as Obliged Entities	n/a	4	n/a	104	309	2	18.450
Other non-financial sector's obliged entities when designated by Member States at national level	n/a	235	n/a	n/a	n/a	n/a	252	n/a	4.307	n/a	450 Pawnbrokers & 15 auction houses	2.195	n/a	n/a	9.778	69	100	n/a	n/a	n/a	n/a	80	17.481

NB: data are based on contributions by Member States (i.e. not all Member States are covered due to non-submissions). Total may not add up due to differences in calculation methods (i.e. total value is only indicative).

ANNEX 5 – STATISTICS ON SUSPICIOUS TRANSACTION REPORTS

Statistics on suspicious transaction reports

Obliged entities are reporting Suspicious Transaction Reports/Suspicious Activities Reports/Unusual Transaction Reports (STRs/SARs/UTRs) depending on the system in place in the Member States (see Eurostat report). In 2015, **701.957** STRs/SARs/UTRs were received from obliged entities based on data collected among 22 Member States (financial sector and non-financial sector).

The following table gives an overview by country and category of reporting entities for the year 2015 (where data were provided).

	Austria	Belgium	Bulgaria	Cyprus	Czech Republic	Denmark	France	Germany	Greece	Finland	Hungary	Italy	Ireland	Latvia	Malta	Netherlands	Poland	Portugal	Slovakia	Slovenia	Spain	Sweden	Total
Financial sector																							
Payment institutions	492	1.274	332	16	108	9.124	4.535	2.253	4575	1.592		3.419		63		11.051	29		53		1.264	3.415	43.595
Currency exchange offices (bureaux de change)		6.601	5		11	535	1.709	0	9	26.464	173	49		314		275.338	153	1.926	86		4		313.377
Credit institutions	1.263	6.711	2.018	456	2.177	98	31.276	25.447	2536	27	7.160	65.935		17.047	136	3.968	71.207	2.307	2.876	441	2.625	5.700	251.411
E-money institutions		17	0		1	37	10	0		0		1.099		17		0	0		0		0	148	1.329
Other financial institutions		0	21	27	22	11	142	459		0	498	2.716		59	11	0	81	133	21		25		4.226
Insurance undertakings	12	891	3		28	1	2.479	149	540	33	357	1.234		0	7	7	976		112	3	11	42	6.885
Investment firms		2	1	51	4	1	140	0	83	3	109	117		0	26	2	71	3	35	2	15	7	672
Collective investments undertakings		1	0				58	0		0		131		0	0	0	89		0		0	3	282
Insurance intermediaries		1	0				65	0		0				4	0	0	0	11	0		0	4	85
Other financial sector's obliged entities		0	29		10			526		41	34	1		0	1	7.083	541	173	0	7	4	482	8.932
TOTAL financial sector	**1.767**	**15.498**	**2.409**	**550**	**2.361**	**9.807**	**40.414**	**28.834**	**7.743**	**28.160**	**8.331**	**74.701**	**21.373**	**17.504**	**181**	**297.449**	**73.147**	**4.553**	**3.183**	**453**	**3.948**	**9.801**	**652.167**
Non-financial sector																							
Lawyers	12	2	2	15	0	7		29		5	2	1.213		11	11	10	19		0	3	24	4	**1.369**
Notaries	4	1.134	5		0		996	1	66	0	8	3.227		3	0	322	11	406	3		252	0	**6.438**
External accountants/auditors	3	205	4	24	0	6	374	3	2	11	23	1.502		0	4	956	1		0		6	13	**3.137**
Tax advisors		2			1			1		0		31		0	0	118	3		0		12	0	**168**
Real-estate agents	1	27	1		2		35	34		8	4	5		0	6	81	2		0		45	3	**254**
Traders in goods receiving cash payments >€15,000	5	-			0	1.331	29	116		103				0	0	4.614	7	32	0		n/a	36	**6.273**
Trust or company service providers		-		11	1			2		0				N/A	34	148	9		0		2	0	**207**
Casinos	1	1.043	5		1	4.435	422	52		0	1	522		0	3	2.364	8	34	0	2	5	313	**9.211**
Providers of gambling services (excl. casinos)		-			na		358	0		9.343		946		0	32	0	0	3.839	22	1	91		**14.632**
Other non-financial sector's obliged entities		0	33	4	2	33	603			73		405			0	159	2	1.275	56	62	217		**2.924**
Other reporting persons														4.697									**4.697**
TOTAL non financial sector	**26**	**2.413**	**50**	**54**	**7**	**5.812**	**2.817**	**238**	**239**	**9.543**	**38**	**7.851**	**312**	**4.711**	**90**	**8.772**	**62**	**5.586**	**81**	**68**	**654**	**369**	**49.793**
TOTAL for financial and non-financial sector	**1.793**	**17.911**	**2.459**	**604**	**2.368**	**15.619**	**43.231**	**29.072**	**7.982**	**37.703**	**8.369**	**82.552**	**21.682**	**22.215**	**271**	**306.221**	**73.209**	**10.139**	**3.264**	**521**	**4.602**	**10.170**	**701.957**

NB: data are based on contributions by Member States (i.e. not all Member States are covered due to non-submissions). Total may not add up due to differences in calculation methods (i.e. total value is only indicative).

In terms of trends concerning the reporting of STRs/SARs/UTRs, Eurostat provides an overview of the period 2008-2010 in its AML/CFT report 2013.

Table 2: Number of reports filed by type

Number of reports filed	2008	2009	2010
STR	88 499	101 341	126 116
SAR	247 366	261 312	266 388
UTR	295 464	90 976	118 559

There is an increase in the total number of STRs and SARs throughout the reference period 2008-2010. This trend is clearly continuing as showed by collected data for 2015 years.

For the reference year 2010, the following data on reporting of STRs/SARs/UTRs per type of obliged entities can be provided:

Table 2: Number of Suspicious Transaction Reports (STRs) filed by each category of obliged entities (2010)

	Reporting Unit	credit institutions	life insurance companies	investment firms	mutual funds	money transfer institutions	bureaux de change	lawyers	notaries	external accounts / auditors	tax advisors	real estate agents	casinos	traders in goods above Euros15000	trusts	company service providers	others	financial institutions	TOTAL
Belgium	STR	3 870	76	0	1	:	11 491	0	163	74	:	26	912	:	:	:	2 060	:	18 673
Bulgaria	STR	726	:	0	0	:	2	1	4	0	0	1	7	0	:	0	117	372	1 230
Czech Republic	STR	1 476	:	:	:	:	:	:	:	:	:	:	:	:	:	:	411	:	1 887
Denmark	STR	968	3	0	0	972	342	4	0	0	3	1	16	0	0	0	7	0	2 316
Germany	STR	10 227	97	0	0	574	0	10	4	0	3	0	11	33	0	0	77	6	11 042
Estonia	STR	2 635	1	0	0	1 744	221	5	59	0	0	0	5	2	0	0	332	29	5 033
Greece	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
France	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
Croatia	STR	307	0	0	2	0	0	5	23	0	0	0	0	:	0	0	63	6	406
Italy	STR	30 345	154	21	30	5 333	24	12	66	18	66	3	34	:	197	:	38	702	37 043
Latvia	STR	22 528	0	0	0	18	2	26	0	0	0	0	1	0	0	0	3 428	:	26 003
Lithuania	STR	165	:	:	:	:	:	:	31	:	:	:	:	:	:	:	26	:	222
Luxembourg	STR	4 629	78	63	:	:	:	13	4	56	2	0	21	0	:	:	:	:	4 866
Hungary	STR	6 551	155	72	0	16	352	0	0	2	0	1	0	2	0	0	0	26	7 177
Malta	STR	38	4	2	0	4	0	3	0	3	0	0	6	0	4	5	4	:	73
Austria	STR	1 941	7	:	:	:	:	12	6	5	:	2	1	3	:	:	241	:	2 218
Poland	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
Portugal	STR	1 061	4	0	0	995	0	0	5	0	0	0	0	2	0	0	138	:	2 205
Romania	STR	1 915	11	:	:	711	1	1	108	:	:	:	1	29	:	:	682	18	3 477
Slovenia	STR	170	0	0	0	0	0	1	1	1	1	1	0	0	0	0	6	0	181
Slovakia	STR	2 031	85	0	0	27	0	1	1	3	2	2	7	0	0	5	192	114	2 470
Sweden	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
Member States reporting Suspicious Activity Reports (SARs)																			
Spain	SAR	2 082	11	14	4	285	:	39	345	6	:	23	7	:	:	:	356	:	3 172
Cyprus	SAR	463	1	8	0	4	:	6	:	2	:	0	:	:	0	2	24	:	510
Finland	SAR	1 000	153	5	:	16 012	:	7	:	17	:	14	3 951	45	:	:	250	:	21 454
United Kingdom	SAR	384	1 430	664	7	8 562	4 216	4 878	:	6 085	:	116	563	3 742	57	:	5 976	204 572	241 252
Member States reporting Unusual Transaction Reports (UTRs)																			
Netherlands	UTR	7 415	2	:	0	108 826	0	11	277	445	127	2	564	44	12	:	834	:	118 559
Member States not providing data																			
Ireland	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
Iceland	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	1	413	414
Liechtenstein	STR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:
Switzerland	SAR	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	1 159
Serbia	STR	:	9	:	:	:	:	:	:	:	:	:	:	:	:	:	63	4 590	4 662
Turkey	SAR	9968	47	2	0	:	11	:	1	:	:	0	:	:	:	:	25	197	10 251

Source: Eurostat (2013)

ANNEX 6 –

EU LEGISLATION RELEVANT IN THE AML/CFT FIELD.

EU legislation on financial services and supervision which is relevant for the AML/CFT field based on article 53 and article 114 TFUE:

- Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.

- Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC repealing Directive 2000/46/EC

- Directive 2010/78/EU of the European Parliament and of the Council of 24 November 2010 in respect of the powers of Supervisory Authority.

- Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

Further EU legislation was adopted in the AML/CFT field based on article 114 TFUE and article 33 relating to controls of cash movements at the external border of the EU:

- Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community (**Cash Control Regulation**).

Other areas relevant to AML/CFT are covered by EU legislation adopted in the CFT field based on article 215 TFUE and article 75 TFUE and 352 TFUE – imposing targeted financial sanctions:

- Council Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.

- Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan.

- Council Regulation (EU) No. 267/2012 of 23 March 2012 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010.

Finally this preventative framework is complemented by EU legislation adopted in the AML/CFT field based on TFUE articles in the area of freedom, security and justice

- Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2000/642/JHA)
- Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime.
- Council Framework Decision of the 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA)
- Council Framework decision on 13 June 2002 on combatting terrorism (2002/475/JHA).
- Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property.
- Framework Decision 2003/577/JAI on freezing of assets and evidence.
- Framework Decision 2006/783/JAI on confiscation.
- Directive 2014/41/EU regarding the European investigation order.
- Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

ANNEX 7 - GLOSSARY

AML/CFT	Anti-money laundering and counter-terrorist financing
API	Authorised Payment Institutions
ATM	Automated Teller Machine
BO	Beneficial Owner
CCTV	Closed-Circuit Television
CCR	Cash Control Regulation
CDD	Customer Due Diligence
CTR	Currency Transaction Report
DNFBPs	Designated Non-Financial Businesses and Professions
EBA	European Banking Authority
ECB	European Central Bank
Egmont Group	the Egmont Group of Financial Intelligence Units (informal international network of FIUs)
E-Money	Electronic Money
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FTF	Foreign Terrorist Fighters
GDP	Gross Domestic Product
IA	Impact Assessment
KYC	Know Your Customer
LEA	Law enforcement authority
MER	Mutual Evaluation Report

ML	Money laundering
MoU	Memorandum of Understanding
MSB	Money Services Business
MVTS	Money Value Transfer Services
NRA	National risk assessment
OCG	Organised Crime Group
PEP	Politically Exposed Person
PSD	Payment Services Directive
RBA	Risk Based Approach
SAR	Suspicious Activity Report
SNRA	Supranational risk assessment
STR	Suspicious Transaction Report
SPSP	Small Payment Services Provider
TBML	Trade-Based Money Laundering
TF	Terrorist financing
TCSPs	Trust and Company Service Providers
UBO	Ultimate Beneficial Owner
UCITS	Undertakings for Collective Investment in Transferable Securities
UTR	Unusual Transaction Report

ANNEX 8 - BIBLIOGRAPHY

1/ Commission's documents

- October 2012 - Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions- Towards a comprehensive European framework for online gambling
  COM (2012) 596 final) and accompanying Commission Staff Working Document (SWD (2012) 345 final

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012DC0596

http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1497268116474&uri=CELEX:52012SC0345

- February 2013 - Final report of the study on the impact of Directive 2007/64/EC on payment services in the internal market drafted on February 2013 by London Economics and *IFF* in association with PaySys.

http://ec.europa.eu/internal_market/payments/docs/framework/130724_study-impact-psd_en.pdf

- July 2014 - Commission recommendation on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0478&from=EN

- October 2014 - Study on the role of regulators for online gambling: authorisation, supervision and enforcement

http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=8180&lang=en&title=Study-on-the-role-of-regulators-for-online-gambling%3A-authorisation%2C-supervision-and-enforcement

- September 2015 - Crowdfunding: Mapping EU markets and events study

https://ec.europa.eu/info/sites/info/files/crowdfunding-study-30092015_en.pdf

- March 2016 – Commission Staff Working Document on the movement of capital and the freedom of payment (SWD(2016) 105)

- July 2016 - Impact assessment accompanying the 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

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0223&from=EN

- November 2016 - Inception impact assessment – Import of cultural goods

http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_taxud_004_cultural_goods_synthesis_en.pdf

- December 2016 - Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0470&from=EN

- January 2017 Inception Impact Assessment - Proposal for an EU initiative on restrictions on payments in cash

http://ec.europa.eu/smart-regulation/roadmaps/docs/plan_2016_028_cash_restrictions_en.pdf

2/ EUROSTAT reports

- Anti-Money Laundering in Europe, Statistical working paper, Eurostat, 2013

http://ec.europa.eu/eurostat/web/products-statistical-working-papers/-/KS-TC-13-007

- Personal remittances statistics, Statistics explained, Eurostat, 25.01.2017

http://ec.europa.eu/eurostat/statistics-explained/index.php/Personal_remittances_statistics

3/ EUROPOL reports

- The European Union (EU) Serious and Organised Crime Threat Assessment (SOCTA), 2013

https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013

- Europol report: why cash is still king?, 2015

https://www.europol.europa.eu/publications-documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering

- Europol 2016, Internet Organised Crime Threat Assessment (IOCTA) 2016

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

- The European Union (EU) Serious and Organised Crime Threat Assessment (SOCTA), 2017

https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

4/ Other Union level bodies

- January 2017 – ESAs Joint Opinion on the risks of money laundering and terrorist financing affecting the Union's financial sector

http://www.eba.europa.eu/documents/10180/1759750/ESAS+Joint+Opinion+on+the+risks+of+money+laundering+and+terrorist+financing+affecting+the+Union%E2%80%99s+financial+sector+%28JC-2017-07%29.pdf

- December 2014 - ESMA opinion - Investment-based crowdfunding

https://www.esma.europa.eu/sites/default/files/library/2015/11/2014-1378_opinion_on_investment-based_crowdfunding.pdf

- EBA Opinion on 'virtual currencies'

https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

- February 2015 – Opinion of the European Banking Authority (EBA) on lending-based crowdfunding

https://www.eba.europa.eu/documents/10180/983359/EBA-Op-2015-03+%28EBA+Opinion+on+lending+based+Crowdfunding%29.pdf

- ECB payment statistics reports

- ECB Consumer cash usage. A cross-country comparison with payment diary survey data

https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf

5/ FATF and Moneyval reports:

- 2009: Money Laundering and terrorist financing risks in the securities sector, FATF

http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20in%20the%20Securities%20Sector.pdf

- 2013: The role of hawala and other similar services providers in money laundering and terrorist financing, FATF

http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

- 2013 (joint report with Egmont): Money laundering and terrorist financing ML and TF through trade in diamonds, FATF

http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

- 2013 - Money Laundering and Terrorist Financing - Vulnerabilities of Legal Professionals, FATF

http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

- 2013 - The use of online gambling for money laundering and the financing of terrorism purposes (Moneyval)

https://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2013)9_Onlinegambling.pdf

- 2015 - Typologies report on Laundering the Proceeds of Organised Crime, Moneyval

http://www.coe.int/t/dghl/monitoring/moneyval/Activities/MONEYVAL(2015)20_typologies_launderingtheproceedsoforganisedcrime.pdf

- 2015 - Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL), FATF

http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

In addition to these sources, general AML/CFT information was used from:

- FATF Typology reports: http://www.fatf-gafi.org/publications/methodsandtrends/?hf=10&b=0&s=desc(fatf_releasedate)

- Moneyval typology reports: http://www.coe.int/t/dghl/monitoring/moneyval/Activities/Typologies_en.asp

6/ Other external information sources

- European Banking sector facts and figures, European Banking Federation, 2015
- Terrorism Financing: Risk Identification and Assessment, IHS Consulting, 15 Septembre 2015
- Terrorism Financing and Money Laundering, Special Report, IHS CONSULTING, 14 June 2016
- Overlaps between terrorism and crime, especially narcotics, Strategic analysis; IHS Consulting, February 2017
- Prospect Analysis Briefing, Cross-border money laundering and terrorist financing: risk assessment, IHS Consulting, 30 January 2015
- Report of the Project 'ECOLEF', The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy, Utrecht University, 2013
- Illicit trade and terrorism financing, Interim note, Centre d'Analyse du Terrorisme, 2016
- Le Financement des Attentats de Paris (Janvier et Novembre 2015), Centre d'Analyse du Terrorisme, 2016
- Assessing the risk of money laundering in Europe – Final Report of project IARM – 31 May 2017 - http://www.transcrime.it/iarm/wp-content/uploads/sites/5/2017/05/ProjectIARM-FinalReport.pdf

7/ Confidential information

Information were received from Europol and EU IntCen (classified)

8/ Oral and written contributions from the following stakeholders

(national associations were represented through their respective European federation)

- Antwerp World Diamond Centre private foundation
- Accountancy Europe
- Association for Financial Markets in Europe
- BEUC – European Consumer Association
- Civil society Europe
- Confédération Fiscale Européenne
- COFACE Family Europe
- Council of the Notariats of the European Union
- Cultural Action Europe
- European Association of Cooperative Banks
- European Association of Public Banks
- European Association of Real Estate Professions
- European Banking Industry Committee
- European Banking Federation
- European Bars (CCBE)
- European Casino Association
- European Foundation Centre
- European Gaming and Amusement Federation
- European Gaming and Betting Association
- European Lotteries
- European Money Association
- European Pari Mutuel
- European Payment Institutions Federation
- Human Security Collective
- Insurance Europe
- International Committee of the Red Cross
- Joint Research Centre on Transnational Crime (TRANSCRIME)
- Law Society of England and Wales
- Leaseurope
- Mastercard
- Moneygram Europe
- Open Society Foundation
- Paypal
- Remote Gambling Association
- STEP
- SWIFT
- University of Sankt-Gallen
- Transparency International EU
- The Council of Bars and Law Societies of Europe

- Trust Europe Affairs (virtual currencies)
- Voice
- Visa
- Western Union Europe