EUROPEAN
COMMISSION

Brussels, 24.7.2019
SWD(2019) 650 final

COMMISSION STAFF WORKING DOCUMENT
Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

{COM(2019) 370 final}

CONTENTS

1. INTRODUCTION

The Financial Action Task Force (FATF) recommends that countries conduct risk assessments that take account of their capacity and experience in each sector subject to requirements on anti-money laundering and countering Terrorist Financing (AML/CFT). They should identify, assess and understand money laundering (ML) and terrorist financing (TF) risks, and take commensurate preventive measures.

Acknowledging the importance of a supranational approach to risk identification, Directive (EU) 2015/849 (4th Anti-money Laundering Directive) mandates the Commission to conduct an assessment of specific ML/TF risks affecting the internal market and relating to cross border activities.

The Commission published its first supranational risk assessment in 2017.[1] Article 6(1) of the 4th Anti-money Laundering Directive also requires the Commission to update its report every two years (or more frequently if appropriate). The current exercise updates the information in the 2017 report, analyses the present ML/TF risks and proposes comprehensive action to address them. It assesses the degree to which the Commission's recommendations for mitigating measures have been implemented and evaluates the remaining risks, taking into account new products and sectors.

The details of the risk analysis for each sector and product are presented in **Annex 1.**

2. METHODOLOGY FOLLOWED FOR THE SUPRANATIONAL RISK ASSESSMENT

This SNRA follows the methodology[2] used for the 2017 SNRA, which provides a systematic analysis of the money laundering and terrorist financing risks linked to the methods used by perpetrators. The aim to identify circumstances in which services and products in a given sector could be abused for ML/TF purposes, without passing judgement on the sector as a whole.

This SNRA focuses on vulnerabilities at EU level, in terms of both the legal framework and its effective application. It presents the main risks for the internal market in a wide range of sectors and the horizontal vulnerabilities that can affect those sectors.

This report sets out mitigating measures that should be taken at EU and national level to address the risks and makes a number of recommendations for the various actors concerned. It does not prejudge the mitigating measures that some Member States have taken or may decide to take in response to national ML/TF risks. The mitigating measures in this report should therefore be considered a baseline that can be adapted, depending on the national measures already in place.

Under Article 6(4) of the 4th Anti-money Laundering Directive, if Member States decide not to apply any of the previous SNRA recommendations, they should notify the

[1] Report from the Commission to the European Parliament and the Council on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM(2017) 340 final.

[2] For more details, see SWD(2017) 241.

Commission of their decision and provide a justification for it ('comply or explain'). No such notification was received to date by the Commission.

Process

In preparing this report, the Commission carried out a broad consultation exercise with all relevant stakeholders, in the course of which it addressed various sectors through targeted questionnaires and dedicated workshops.

The Commission consulted the Member States by means of a questionnaire in July 2018, with enclosures on:

- national mitigating measures;
- templates for financial and prosecution ML/TF data; and
- emerging risks.

By the end of 2018, the Commission had received 23 replies.[3] Subsequently, Member States were further consulted in dedicated meetings of the Expert Group on Money Laundering and Terrorist Financing[4] on 10 December 2018 and 11 February 2019.

In November-December 2018, the Commission held four workshops with private-sector stakeholders, one with representatives of financial institutions, two with 'designated non-financial businesses and professions' (DNFBPs)[5] and one with civil society (NPOs) and academics. A second phase of this round of meetings took place in January 2019. The oral input from the private sector was complemented by 15 written replies.

The Commission also consulted other regulatory agencies and authorities, such as Europol and the European supervisory authorities (ESAs).[6]

The purpose of this broad consultation was twofold: to follow up on the recommendations made in the 2017 and to update the supranational risk assessment.

Finally, given the evolving nature of ML/TF threats and vulnerabilities, the supra-national risk assessment needs to take an integrated approach to assessing the effectiveness of national AML/CFT arrangements.

In order to monitor their compliance with EU requirements, their implementation and their preventive capacity, the Commission takes due account of national risk assessments (NRAs) produced by the Member States to ensure the proper identification and mitigation of specific national risks.[7]

---

3 BG, CY, FR, HR and IE did not reply to the questionnaire on the follow up of recommendations.

4 This group is made up of senior civil servants responsible for AML in the EU/EEA countries; http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2914

5 Representatives of the gambling industry were consulted in a separate meeting.

6 The European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

7 This is without prejudice to evaluations by relevant international organisations and standard setters, such as FATF and the Committee of Experts on the Evaluation of Anti-Money Laundering Measures

Individual sectors are responsible for a third layer of risk assessment that takes account of risk factors, including those relating to specific customers, countries, products, services, transactions and delivery channels.

These three layers (supranational, national and sectoral) of risk assessment, along with risk mitigation, where appropriate feed into a comprehensive awareness and analysis of ML/TF risks in the EU in which different layers complement each other and are equally relevant.

The Commission draws on and complements national and sectoral assessments by assessing risks that affect the Union internal market and are related to cross border activities.

The legal framework

The risk assessment needs to provide a snapshot of the money laundering and terrorist financing risks and requires a clear-cut timing. The assessment of risks affecting the EU was carried out at a time when the relevant legislative framework was still the 4th Anti-money Laundering Directive. Even though the 5th Anti-Money Laundering Directive was adopted, its transposition has not been completed yet.

Therefore the supranational risk assessment is based on the EU legislation implemented at the time of the assessment. This is particularly important to stress since some sectors were not, or only limitedly, covered by the obligations in the 4th Anti-money Laundering Directive. Therefore the risk level may be assessed differently for those Member States having already applied the stricter regime. Nevertheless, changes brought by the 5th Anti-Money Laundering Directive to be transposed by January 2020 have been anticipated when defining the new mitigating measures.

While the main EU instrument is the Anti-money Laundering Directive, the Union's anti-Money Laundering and Countering Terrorist Financing legal framework is complemented by other EU legislation. An indicative list is attached in **Annex 2.**

In addition, an index of abbreviations used in the risk analysis is attached in **Annex 3** and a bibliography in **Annex 4**.

3. OUTCOMES OF THE SUPRANATIONAL RISK ASSESSMENT

This supranational risk assessment focuses on the risks associated with each relevant sector and assesses the recommendations made to address the concerned risks. The Commission identified **47 products and services** that it regards as potentially vulnerable to ML/TF risks at the level of the internal market, up from 40 in the 2017 assessment. These 47 products and services concern **11 sectors**, including:

(Moneyval). Moneyval is a permanent monitoring body of the Council of Europe. It assesses compliance with the principal international AML/CFT standards and the effectiveness of their implementation, and makes recommendations to national authorities on how to improve their systems; https://www.coe.int/en/web/moneyval

- the 10 sectors or products identified in the 4th Anti-money Laundering Directive, i.e. credit and financial institutions, money remitters, currency exchange offices, high-value goods and assets dealers, estate agents, trust and company service providers (TCSPs), auditors, external accountants and tax advisors, notaries and other independent legal professionals, and gambling service providers;
- 1 category of various different products not covered in the 4th Anti-money Laundering Directive, but considered relevant for the risk assessment, that encompasses cash-intensive businesses, virtual currencies, crowdfunding and non-profit organisations. This category also covers certain informal means, such as those used by Hawala[8] and other informal value transfer service providers; and
- four new products/services that were not assessed in the 2017 report, namely privately owned automated teller machines (ATMs), professional football, free ports; and investor citizenship and residence schemes ('golden passports/visas').

In addition, this report contains an enhanced analysis of some services that were assessed in the 2017 report, namely FinTech; virtual currency exchange platforms and wallet providers; and bank accounts of non-residents.

The descriptions and the assessments of many of the products/sectors analysed in the 2017 report have not been fundamentally modified over the last two years, while the revised Union AML/CFT legal framework has been significantly updated since 2017.

This assessment updates the information in the 2017 report, fine-tuning it in several areas (such as non-profit organisations /NPOs), and updating figures and information sources. Also, this assessment is updated to include reference to the current Union AML/CFT legal framework, taking into account that most of the recommendations for mitigating measures in the 2017 SNRA[9] are now included in the 5th Anti-money Laundering Directive. Moreover, special attention was paid to Member States' implementing measures of the 4th Anti-money Laundering Directive, which had to be transposed by July 2017. Other mitigating measures recommended in the 2017 SNRA are currently accounted for by recent EU legislation such as Directive on company law[10] or the new Cash Control Regulation.[11]

---

[8] Hawala is a popular and informal value transfer system based on the performance and honour of a huge network of money brokers ('hawaladars'), rather than the movement of cash.
Informal value transfers take place within systems or networks that receive money for the purpose of making funds or an equivalent value payable to a third party elsewhere, whether or not in the same form. They generally take place outside the conventional banking system.

[9] Some of which were drafted in the light of the Regulation 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, p. 15–36.

[10] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law, OJ L 169, 30.6.2017, p. 46). This Directive 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. 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. 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.

[11] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation No 1889/2005/EC, OJ L 284,

ANNEX 1 – RISK ANALYSIS BY PRODUCT/SECTOR

This SNRA has followed a specific methodology involving systematic analysis of the ML/TF risks linked to perpetrators' methods. The aim is to identify the circumstances under which the services and products a given sector provides could be abused for ML/TF purposes (without passing judgment on a sector as a whole).

It is based on Directive (EU) 2015/849 (4th Anti-money Laundering Directive), which was the legislation in force at the time of the analysis. The 5th Anti-money Laundering Directive (Directive (EU) 2018/843) which amended the 4th Anti-money Laundering Directive, is considered part of the mitigating measures.

Each risk is rated for threat and vulnerability. The ratings are on a scale from 1 to 4, as follows:

1) **low significance (value: 1)**
2) **moderately significant (value: 2)**
3) **significant (value: 3)**
4) **very significant (value: 4)**

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

12.11.2018, p. 6–2. This Regulation complements the EU's legal framework for the prevention and terrorist financing laid down in Directive 2015/849. It addresses areas in which an evaluation of Regulation (EC) No 1889/2005 (the Cash Control Regulation) identified room for improvement and implements a number of action points set out in the Commission's Action Plan for strengthening the fight against terrorist financing, COM(2016) 50 final, 02.02.2016.

CASH PRODUCTS

1. 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.

The evolution of the international standards to control cross-border flows of cash, the evaluation of the extent to which this Regulation achieved its objectives, and the information received from Member States led the Commission to conclude that, while the overall performance of the Regulation was satisfactory, a number of areas should be strengthened to improve its functioning.

In order to address these areas, and as part of the European Agenda on Security and Action Plan for strengthening the fight against terrorist financing, the Commission adopted a proposal for a new Cash Controls Regulation in December 2016. Following the legislative work with the European Parliament and the Council, the new Regulation (EU) No 2018/1672[12] was adopted in October 2018 and will enter into application in June 2021.

Currently in application, the Cash Control Regulation (Regulation (EU) 1889/2005)[13]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).

[12] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation No 1889/2005/EC, OJ L 284, 12.11.2018, p. 6–2.
[13] Regulation No 1889/2005/EC, OJ L 284, 12.11.2018, p. 6–2.

Current rules on the movement of cash in and out of the EU have applied since 15 June 2007 and are an integral part of the EU's Anti Money Laundering and Terrorist Financing framework. The new Regulation updates these rules and complements the EU's legal framework for the prevention of money laundering and terrorist financing set out in Directive 2015/849 as amended by Directive 2018/843.

The new Cash Control Regulation, which will enter into application in 2021, improve the existing system of controls on cash entering or leaving the EU – the latest developments in international standards on combating money laundering and terrorism financing developed by the FATF will be reflected in EU legislation.

Under the new Regulation, the definition of cash has been extended to cover not only currency and bearer negotiable instruments but also highly liquid commodities such as gold. The Regulation is also extended to cover cash that is sent by post, freight or courier shipment. In addition it enables Customs authorities to act on amounts lower than the declaration threshold of EUR 10 000, where there are suspicions of criminal activity while improving the exchange of information between authorities (Customs and Financial Intelligence Units) and Member States.

The new legislation extends the obligation of any traveller entering or leaving the EU and carrying cash to a value of EUR 10 000 or more to declare it to the customs authorities. The declaration will be required irrespective of whether travellers are carrying the cash in person, in their luggage or means of transport. At the request of the authorities they will have to make it available to be checked.

If the cash is sent by other means ("unaccompanied cash"), the relevant authorities will have the power to ask the sender or the recipient to make a disclosure declaration. The authorities will be able to carry out controls on any consignments, packages or means of transport which may contain unaccompanied cash.

Member states will exchange information where there are indications that cash is related to criminal activity which could adversely affect the financial interests of the EU. This information will also be transmitted to the European Commission.

In addition the new Cash Controls Regulation provides in its Article 5 (4) that the risk assessments produced by the Commission and by FIUs should be taken into account by Customs authorities when establishing the common risk criteria framework for performing controls.

The new regulation will not prevent member States from providing additional national controls on movements of cash within the Union under their national law, provided that these controls are in accordance with the Union's basic freedoms.

Per year, on average 90 000 cash declarations are submitted, representing a total amount of around EUR 52 million. Customs controls detect 12,000 cases where cash was not declared representing around EUR 345 million per year.

General comment

This risk scenario is intrinsically linked to use of/payment in cash and to high value denomination banknotes risk scenario.[14]

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, road 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

[14] See, in general, the report (2015) by EUROPOL *Why is cash still king?:* https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf

compactness. Cash transportation has been a recurring modus operandi for terrorist groups in Syria– 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 separately below).

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 analysed below).[15]

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 modus 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

FATF Report: Money laundering through the physical transportation of cash (October 2015)[16]

Based on the working paper of the European Central Bank – consumer cash usage – a cross country comparison with payment diary survey data,[17] the report noted that in the countries surveyed, between 46 % and 82 % of all financial transactions are conducted in cash, namely Australia (65 %), Austria (82 %), Canada (53 %), France (56 %), Germany (82 %) the Netherlands (52 %), and the United States of America (46 %).[18]

With regard to an economy linked to transnational organised crime, the report pointed to physical transportation of cash across an international border, which is 'one of the oldest

[15] The New Cash Controls Regulation that will enter into force in June 2021 will also cover gold. For prepaid cards, if there is strong evidence that prepaid cards are being used by criminals to transfer value across the EU borders circumventing the legislation then a delegated act might be used to include prepaid cards within the scope of the Regulation.
[16] http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf
[17] https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf
[18] ECB Working Paper, No 1685/June 2014, Table 1, p. 38.

and most basic forms of money laundering' and is also used for terrorist financing.[19] Although there is no reliable data on the amount of money 'laundered' in this way, the report estimated its volume to be between 'hundreds of billions and a trillion US dollars per year'. The report explained that the most frequently encountered and 'laundered' currencies are stable and widely used currencies such as the US dollar, the euro, the Swiss franc and the British pound, usually, with high denomination notes used. The report also highlighted that criminals exploit the existing cash declaration systems mechanisms, for example, by 'reusing cash declarations several times for the same purpose'.[20]

In the 2015 Europol report *Why cash is still king?,* law enforcement investigations confirm that cash, and in particular high denomination notes, are commonly used by criminal groups as a facilitator for money laundering. Operations themselves reveal huge sums of cash moved and stashed by criminals which are steadily invested and integrated in the legal economy in a multitude of ways which rid them of bulky cash holdings at risk of being confiscated. These methods require an army of criminal associates and complicit or negligent gatekeepers to ensure that their insertion in the legal economy doesn't arouse suspicion.

In the EU, the use of cash is still the main reason triggering suspicious transaction reports within the financial system, accounting for 34% of all reports.

Criminals who generate 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, perhaps due to the predominant use of cash in some jurisdictions' economies, more lax supervision of the financial system or stronger banking secrecy regulations, or because they may have greater influence in the economic and political establishment.

Cash smuggling may occur at other stages and is also used by non-cash generating offences. For example cybercrimes such as phishing and hacking make use of money mules to receive and withdraw sums fraudulently obtained from victims' bank accounts in cash. These funds are thereafter sent via wire transfer to other jurisdictions where they are collected in cash by a select number of individuals, likely for onward transportation.

Since 2017, cash has remained a relevant threat in regards to money laundering. European investigations indicate that movements of cash inside the EU and outside are associated with criminal offences. The most relevant crime area is drug trafficking. Drug related cash proceeds generated through the sales and distribution of predominantly cocaine and hashish are accumulated and received by the designated collectors. The drug trafficking organizations (DTO) then engage with money brokers (traditionally outside of the EU), these brokers charge a commission for facilitating towards the DTOs the value of their proceeds. The brokers dispose of their own laundering networks in different countries. After the arrangement is made, the cash collectors deliver the cash proceeds to the designated intermediaries. From there the cash starts moving, crossing the EU towards the designated exit point or exiting directly the EU. The current legal framework

[19] FATF report. p. 3.
[20] ibid., p. 16.

in the EU has significantly hindered the opportunities for introducing into the financial system large amount of illegal drug proceeds. Because of this, money is used in Trade-Based Money Laundering (TBML) schemes[21] or is transported out of the EU towards "cash friendlier" jurisdictions. Dubai and Beirut have in the last years shown steady presence as preferred cash destinations and growing financial hubs in the EU.

The cash couriers are associated with the threat of the large denomination banknotes: 500 and 200 Euro.

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, which is now covered by the new regulation – 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) and the new regulation extends these customs controls to cash sent in postal parcels or freight shipments, to prepaid cards and to precious commodities such as gold, which were not previously subject to customs control. 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.

Where unaccompanied cash is concerned (cash sent through consignments or parcels) the new regulation enables the competent authorities to request the sender or the recipient, as

[21] TBML is the process by which criminals use a legitimate trade to disguise their criminal proceeds from their unscrupulous sources. The crime involves a number of schemes in order to complicate the documentation of legitimate trade transactions; such actions may include moving illicit goods, falsifying documents, misrepresenting financial transactions, and under- or over-invoicing the value of goods.

the case may be, to make a disclosure declaration. The declaration will be done in writing or electronically using a standard form. The authorities will also have the power to carry out controls on any consignments, receptacles or means of transport which may contain unaccompanied cash.

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 new regulation allows the competent authorities to carry out risk analysis and concentrate their efforts on those shipments which they deem to present the highest risk, while not imposing systematic additional formalities. The disclosure obligation is subject to a threshold identical to that for cash carried by natural persons.

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 new Cash Controls Regulation, applicable from 3 June 2021, reinforces the existing rules on cash movements:

- It enables authorities to act on amounts lower than the declaration threshold of EUR10 000, where there are suspicions of criminal activity,

- Improves the exchange of information between authorities and Member States;

- Enables competent authorities to demand disclosure for cash sent in unaccompanied consignments such as cash sent in postal parcels or freight shipments;

- Extends 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.

2. Cash intensive business

Product
Cash intensive business

Sector
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, strip clubs, massage parlours.

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 *Trends and developments in the use of euro cash over the past ten years*[22] (published as part of the ECB Economic Bulletin, Issue 6/2018).[23]

On 2 February 2016, the Commission published a Communication to the European Parliament and the Council on an Action Plan to further step up the fight against the financing of terrorism.[24] The Action Plan built on existing EU rules in order to adapt to new threats and aimed to update EU policies in line with international standards. It discussed numerous issues and solutions in different fields related to terrorism financing.

In the context of the Commission's action to extend the scope of the Regulation on controls of cash entering or leaving the European Union, reference was made to the appropriateness of exploring the relevance of potential upper limits to cash payments.[25] The Action Plan also further noted that "Several Member States have in place prohibitions for cash payments above a specific threshold". However, such prohibitions have not been considered at EU level.

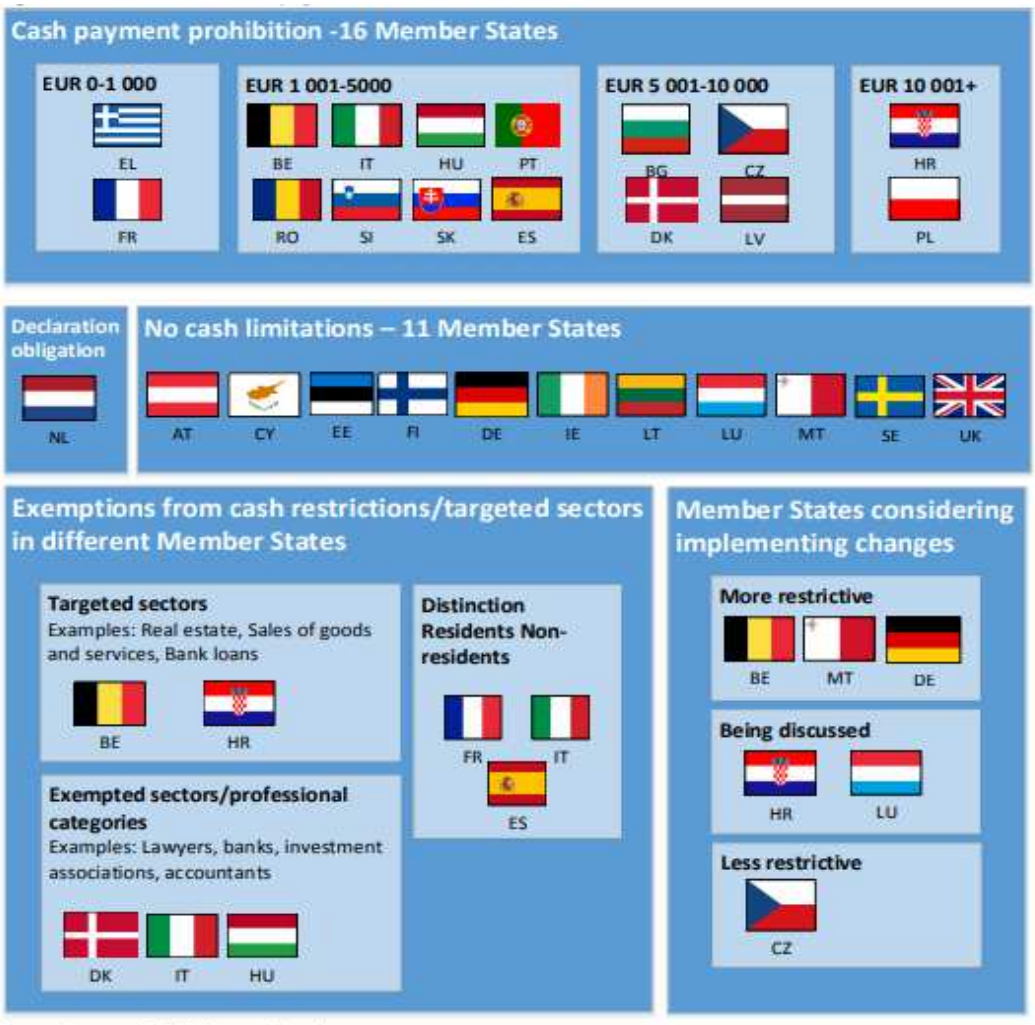
The figure below outlines the cash payment restrictions currently in place in the EU Member States, as well as whether there are plans to adapt or change them. The first infographic shows that currently cash prohibition are enforced in 16 EU Member States. The thresholds vary from EUR 500 in Greece and EUR 1 000 in France to approximately EUR 13 800 in Croatia and EUR 15 000 in Poland. The Netherlands is the only country that has adopted a declaration obligation and the remaining 11 EU Member States do not have any cash limitations in place.

In several EU Member States particular business sectors or consumers are exempted or targeted by the cash prohibitions. In France, Italy and Spain a distinction is made between residents in the respective countries and non-residents. In this sense, in France and Spain non-residents can perform payments up to a higher threshold (EUR 15 000),

[22] https://www.ecb.europa.eu/pub/economic-bulletin/articles/2018/html/ecb.ebart201806_03.en.html#toc2
[23] https://www.ecb.europa.eu/pub/economic-bulletin/html/eb201806.en.html
[24] COM (2016)50.
[25] The Action Plan stated that "Payments in cash are widely used in the financing of terrorist activities… In this context, the relevance of potential upper limits to cash payments could also be explored. Several Member States have in place prohibitions for cash payments above a specific threshold".

while in Italy, the general threshold is not applicable for non-residents. Other countries exclude from the cash restrictions particular sectors enabling professionals in those sectors perform transactions in cash above the generally applicable threshold. For instance in Denmark eleven professional categories including banks and lawyers, are exempted from the thresholds. In the cases of Belgium and Croatia, certain lower thresholds apply in certain sectors. For instance in Belgium cash transactions are completely banned in the real estate sector.

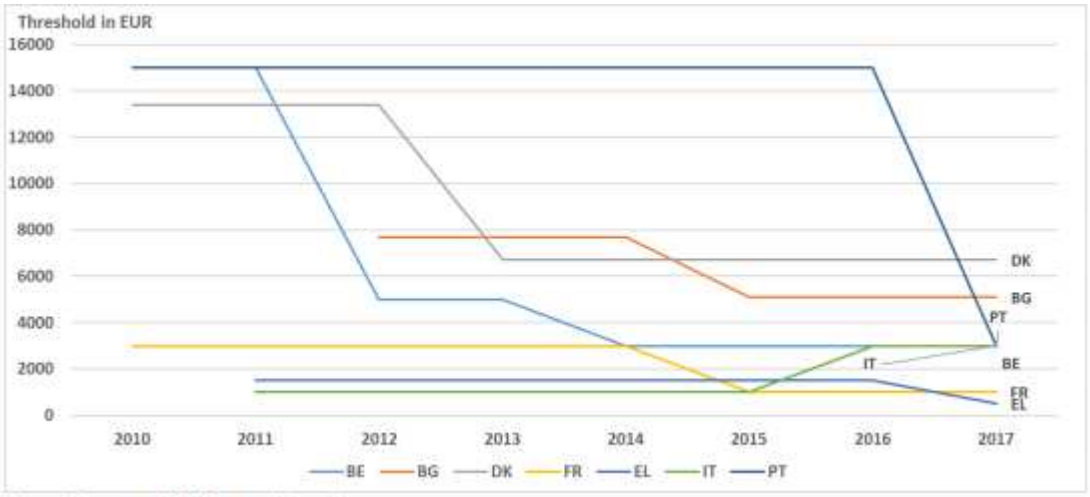
Adoption of new cash payment prohibition is discussed in a number of countries, while others are considering of changing their current threshold. Belgium is considering expanding the scope of the restrictions and including all operations apart from individuals. Germany and Malta are considering adopting a cash payment prohibition. The issue is also discussed in Luxembourg and Croatia, without a concrete proposal for either more or less restrictive measures being prepared. The Czech Republic is the only country considering to move towards less restrictive measures.



Source: Ecorys and CEPS own elaboration.

The figure below indicates that six of the EU Member states, which have a cash payment prohibition in place, have lowered the threshold in the last seven years. Italy is the only

EU Member State which adopted a cash payment prohibition at a lower threshold (EUR 1 000) and then raised it in 2016 to EUR 3 000.



Source: Ecorys and CEPS own elaboration.

Description of the risk scenario

Cash-intensive businesses are 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

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, etc. 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.

LEAs confirm that cash intensive businesses continue to be used to launder criminal proceeds.

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

Currently no upper limits to cash payments are in place at the EU-wide level. In its Action Plan for strengthening the fight against terrorism financing, the Commission already signalled upper limits to cash restrictions could be further explored as an additional initiative to complement the current European AML/CFT framework.[26]

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

[26] See COM2015(50).

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 suspicious transactions reports (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.

To increase vigilance and mitigate the risks posed by such cash payments, persons trading in goods are covered by the Directive to the extent that they make or receive cash payments of EUR 10 000 or more. This same threshold is further referred to by Directive 2018/843 (the 5th AML Directive). Member States are able to adopt lower thresholds, additional general limitations to the use of cash and further stricter provisions.

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 customer due diligence (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 examined whether 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.[27] 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 and especially money-laundering related activities,[28] as the need to use non anonymous means of payment would either deter the activity or contribute to its easier detection and investigation. The report arrived to the conclusion that no further legislation in this regard would be proposed for the moment now.

- 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 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.

[27] A report from the Commission to the European Parliament and the Council on restrictions on payments in cash (COM(2018) 483 final) was presented on 12 June 2018.

[28] It's worth noting that the above-mentioned Commission's report suggests that *"...restrictions on payments in cash would not significantly prevent terrorism financing, but indicated that such restrictions could be useful in combatting money laundering."*

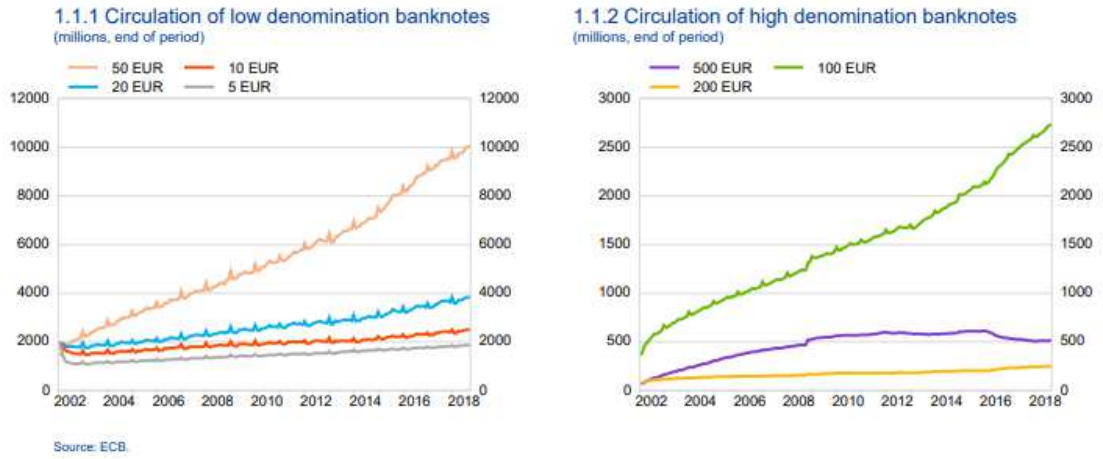
3. High value banknotes

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.



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.

On 4 May 2016, the Governing Council of the European Central Bank (ECB) decided to discontinue the production and issuance of the EUR 500 banknote. It did so taking into

account the concerns of Europol[29] and many Member States that this is a banknote that facilitates illicit activities. Based on the ECB's decision, since 27 April 2019, the banknote has no longer been issued by central banks in the euro area, but continues to be legal tender and can be used as a means of payment.

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

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 keen on 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 the 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 law enforcement authorities (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.

Operations themselves reveal huge sums of cash moved and stashed by criminals which are steadily invested and integrated in the legal economy in a multitude of ways which

[29] https://www.europol.europa.eu/newsroom/news/europol-welcomes-decision-of-ecb-to-stop-printing-eur-500-notes

rid them of bulky cash holdings at risk of being confiscated. These methods require numerous criminal associates and complicit or negligent gatekeepers to ensure that their insertion in the legal economy does not arouse suspicion.

In the EU, the use of cash is still the main reason triggering suspicious transaction reports within the financial system, accounting for 34% of all reports.

Criminals who generate 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, perhaps due to the predominant use of cash in some jurisdictions' economies, more lax supervision of the financial system or stronger banking secrecy regulations, or because they may have greater influence in the economic and political establishment.

Cash smuggling may occur at other stages and is also used by non-cash generating offences. For example cybercrimes such as phishing and hacking make use of money mules to receive and withdraw sums fraudulently obtained from victims' bank accounts in cash. These funds are thereafter sent via wire transfer to other jurisdictions where they are collected in cash by a select number of individuals, likely for onward transportation.

The cash couriers are associated with the threat of the large denomination banknotes: 500 and 200 Euro. These banknotes are not used as a legal tender and in fact in Europe in many locations they are not accepted as payment. The high denomination banknotes are used by criminals to store value or for transportation (decreased volume of high overall amount). For example, the safety deposit box of a Belgian underground operator identified during the investigation of laundering hashish proceeds of Moroccan organised criminal groups revealed predominantly 500 and 200 banknotes in overall value of 1 600 000 Euro.

Counterfeit euro banknotes continue to be trafficked in bulk on lorries, and by couriers. Post and parcel services are increasingly used to distribute counterfeit euro banknotes sold via online platforms. Currency counterfeiters continue to introduce counterfeit banknotes into circulation by purchasing low-value goods with high-value banknotes to receive legitimate currency in exchange.

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 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 financial intelligence units (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 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. 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.

Conclusions: 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 very significant (level 4).

Mitigating measures

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

4. Payments in cash

Product
Payments in cash

Sector
/

General description of the sector and related product/activity concerned

The European Central Bank (ECB) has conducted a comprehensive study[30] to analyse the use of cash, cards and other payment instruments used at points of sale (POS) by euro area consumers in 2016. The survey results show that in 2016 cash was the dominant payment instrument at POS. In terms of number, 79% of all transactions were carried out using cash, amounting to 54% of the total value of all payments. Cards were the second most frequently used payment instrument at POS; 19% of all transactions were settled using a payment card. In terms of value, this amounts to 39% of the total value paid at POS.

Thus it unquestionably remains the payment method of choice among consumers for low value transactions (i.e. less than 20 EUR).

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 by justifying its origin based on fictitious economic activities (both for goods and services). Terrorists may finance, through often

[30] *The use of cash by households in the euro area,* ECB Occasional Paper Series No 201 / November 2017: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op201.en.pdf

small amounts of cash, terrorist activities without any traceability (see general description under cash intensive business).

General comment

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.

Illegal cash is supplied to intermediaries to buy goods in countries with no or few restrictions on cash payments. Products purchased either hold considerable value, such as luxury goods, or for which there is a specific but considerable demand: such as vehicles (whether second-hand or luxury, construction machineries).

Cash integration by buying from legitimate trading companies goods that are exported at market price is increasing.

Conclusions: based on the feedback from law enforcement authorities (LEAs) and financial intelligence units (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 4th AML Directive provides that high value dealers accepting payment in cash beyond EUR 10 000 are subject to AML/CFT rules and have to apply customer due diligence (CDD) requirements. This obligation applies to any persons trading in goods when the payment is made in cash beyond EUR 10 000 – but it does not cover services, apart from gambling services, and in that case when carrying out transactions amounting to EUR 2 000. These same thresholds are followed by Directive 2018/843 (the 5th AML Directive).

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 currency transactions reports (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.

Conclusions: 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 very significant (level 4).

Money laundering

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 law enforcement authorities (LEAs) and financial intelligence units (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 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 NRA the risks posed by payment in cash in order to define appropriate mitigating 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.

5. Privately owned ATMs

Product
Privately owned ATMs

Sector
/

General description of the sector and related product/activity concerned

A possible misuse of cash machines (ATMs) for money laundering purposes has been brought to the attention of LEAs. According to information received the legal possibility for private parties to buy and rent ATMs from wholesale suppliers is creating a loophole that criminals are taking advantage of.

For many merchants, owners of clubs, bars and restaurants installing one of these ATMs has proven to be a business oriented decision – the client is offered the convenience to withdraw cash and the merchant is maximizing the probability that some of that cash will be spent in his business.

Description of the risk scenario

a) ATM loading options

In order to load the machine one option is to use the services of cash management/cash delivery company.

Another option for the merchant operating a business is to load the cash from his teller. This provides additional opportunities for traders to commit tax evasion by selling goods in exchange of cash without issuing receipts. They then simply place their black cash inside their ATM machine and wait for it to be taken by normal clients. At the end of the year such sales are never declared to their tax authority

The third and most concerning option is simply to load the ATM with criminal cash. Intelligence gathered shows that in cases where criminal cash is used the modus operandi is the following: a courier delivers to the ATM owner/merchant criminal cash. It may derive from different cash generating activities like drug trafficking, illegal immigration, trafficking in human beings, labour and sexual exploitation, selling of counterfeit of smuggled goods, theft, robbery, etc. The criminal cash is then loaded into the machine. As unsuspecting customers or passers-by in need of cash are using their cards to withdraw cash the same amount is debited from their bank accounts and credited into the account of the owner of the ATM/merchant. Afterwards, he can simply transfer the money to any given account controlled by the criminal, minus the commission agreed upon.

b) De-linking bank accounts and internationalization risks

An internationalized, potentially much more dangerous risk scenario appears when national regulations require that a private entity buying an ATM should upon its purchase provide a national bank account number which is linked to the ATM and its activities, but there is no requirement for the merchant to request cash for the ATM from the same bank account that he linked to his ATM or even from the same bank.

A review of the companies offering private ATM services shows that there are several major suppliers, British and American,[31] who have managed to make their business international.[32]

Important questions arise concerning the accounts to which these ATMs (sold by EU and US companies and present in EU countries) are linked. If they are linked to an EU national bank account, but physically present in another country, then it is virtually impossible to establish the origin of the cash being inserted in them.

c) Tax evasion and fraud

Private ATMs are also used for tax evasion and fraud especially as some cash-intensive business operators encourage their clients to extract cash for services that are not invoiced or recorded. The amount of money lost in tax revenues from tax evasion and fraud through private ATMs is more significant than the amount laundered.

d) Micro-structuring by organized crime

With respect to money laundering, private ATMs are often used to "microstructure" – depositing and withdrawing of small sums of money that are consistent with normal ATM withdrawal amounts, going undetected by bank controls. Organized crime members will make voluminous small daily cash deposits into 100 or more bank accounts using private ATMs to avoid triggering anti-money laundering reporting requirements.

General comment

Private ATMs tend to be located in cash-intensive businesses. In addition, privately owned ATMs can also be found in money service businesses (MSB). Taking into consideration the fact that the presence of an ATM in a MSB is illogical due to the nature of an MSB service and also the fact that many hawaladars'[33] side legal business is

[31] As an example: YourCash Europe – a company that controls 32% of the free-to-use ATM market in the UK – has branches in The Netherlands, Belgium and Ireland as well as ATMs in additional jurisdictions. In addition Cardtronics (some branches operating under the trademark DC Payments) operates in 11 countries. Besides the mentioned branches out of Europe (South and North America, New Zealand and Australia, South Africa) and the UK branch, they operate in Ireland, Germany, Poland and Spain.

[32] As an additional example, the ATM locator section of the LINK website: (https://www.link.co.uk/consumers/locator/) shows that there exist privately owned UK ATMs physically present in Belgium, Czech Republic, France, Germany, Gibraltar, Italy, Netherlands, Ireland and Switzerland, as well as Guernsey, Isle of Man and Jersey.

[33] See the section on "Hawala".

running an MSB or a currency exchange service, the risk of misuse can be clearly identified.

Threat

Terrorist financing

There exist currently few especific assessments of the TF threat related to privately owned ATMs. Nevertheless, the combined assessment on payments in cash as well as the analysis on cash couriers show that this modus operandi is widely accessible and low cost.

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. Cases have been identified concerning low amounts and involving integration of cash carried from third countries into the financial system/legal economy of the EU (analysed in a separate section of this report).

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 privately owned ATMs shows that this modus operandi is exploited by criminals as it represents a viable option which is rather attractive and secure. It constitutes an easy way to evade taxes and 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: 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 the TF vulnerability related to privately owned ATMs shows that the main factors are linked to the risk posed by cash.

a) risk exposure
The vulnerability assessment of TF related to privately owned ATMs is intrinsically linked to the assessment related to the use of/payments in cash in general and can follow the same rationale. Privately owned ATMs allow the processing of a huge number of anonymous transactions which require but an initial investment. Hence it has a high inherent risk exposure.

b) risk awareness
The risk awareness appears to be quite low.

c) legal framework and controls in place
The legal frameworks in place vary from one Member State to another and, thus, controls can potentially be inexistent.

Conclusions: **the vulnerability of privately owned ATMs is intrinsically linked to the vulnerabilities related to the use of cash in general.**
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 is considered as very significant (level 4).

Mitigating measures

Private ATM companies pose an increased risk to banks and should be treated as high-risk in money laundering compliance risk assessments. The risks for banks are not just financial but reputational.

- Firstly, customers who have privately owned or operated ATMs should be duly identified.

- Once the bank has identified an ATM owner or operator, it should obtain additional information to gain an understanding about the ATM owner/operators well as an understanding of the ATM owner's procedures.

- After sufficient information is obtained, the sponsoring bank should implement a process to monitor the accounts of the ATM owners. The information obtained during the due diligence process should enable the bank to determine the amount of monitoring necessary as well as how often.

- Member States should guarantee the obligation to register, limit ownership, monitor, or examine privately owned ATMs – up to and including the obligation to link ATMs to a bank account of the Member Sate they are physically located in.

1. 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 since 1998, domestic or euro area deposit liabilities in the EU rose by 3.1% to €23.6 trillion in December 2017 (€17.5 trillion in the euro area and €5.3 trillion in the rest of the EU Member States). This was the highest level recorded, with the previous peak at €23.1 trillion in 2012. Deposits from other monetary financial institutions (MFIs) rose for the first time since 2011 to €7.1 trillion.

Total deposits from non-monetary financial institutions, excluding central governments, grew by 2.5% in 2017 to €16.3 trillion in the EU at the end of 2017, with €12.1 trillion in deposits coming from the euro area.

Growth has been driven by an increase in deposits from households, which rose by 2.9% year on year to €9.1 trillion, and from non-financial corporations (NFCs), up by 6.7% to €3.2 trillion.

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 or criminal sources into the financial system with a view to using it for terrorist purposes.

Money mule mechanisms may be used to transfer proceeds out of the banking sector using personal accounts, either through cybercrime (scamming, fake banking websites etc.) or through money value transfer services.

'Bridge accounts' are also used to launder money. These are accounts of legal or natural persons in the EU with the sole purpose of transferring funds to non-EU countries.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to deposits on account shows that this risk scenario concerns both the placing and withdrawing of funds (i.e. deposits on

account and use of this account withdrawing those funds or transferring to another bank accounts).

Account deposits are frequently used by terrorists, but also by relatives/friends; this extends the scope of the intent and capability analysis.[34] 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 generally withdraw bank account deposits through ATMs located in high-risk non-EU 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. Anyhow, the use of deposit accounts for TF purposes may, in conflict zones, be complicated by difficulties to access funds, especially where access to ATMs or a functioning banking network is disrupted. The source of the funds deposited on bank accounts may come from both legitimate and non-legitimate origins.

In general, using deposits accounts 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 experience 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. This 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 makes this risk scenario rather attractive.

Conclusions: terrorists groups rather frequently use deposits on account to easily enter cash in bank accounts and withdraw money for terrorist activities, although it requires some basic knowledge and planning capabilities to ensure that funds deposited appear legitimate. As a result, this method is rather attractive for terrorist groups. That being the case, the level of terrorist financing threat related to deposits on accounts is considered as significant/very significant (level 3/4).

Money laundering

The assessment of the money laundering threat related to deposits on account shows that this risk scenario concerns both the placing and withdrawal of funds (i.e. deposits in an

[34] The intent and capability analysis is described in the methodology:

- 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.

account and subsequent use of this account, withdrawing money from that deposit account or transferring money to disguise the origin of funds).

Deposits on account are frequently used by organised crime organisations, but also by relatives/close associates, which extends the scope of the intent and capability analysis.[35] Law enforcement authorities report frequent use of this method since it is one of the easiest ways to integrate illicit funds into the financial system. Although in the case of small amounts of money, deep planning and knowledge of how banking systems work may not be necessary, in the case of a complex money laundering case involving funds deposited on accounts transiting via a chain of complex operations, more in-depth knowledge is necessary and perpetrators may use available expertise from intermediaries.

Conclusions: In the light of the above threats, specially the use by criminal organizations, the level of the money laundering threat related to deposits on account is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of terrorist financing vulnerability related to deposits on looked at the placement and withdrawing of funds

a) risk exposure

Banks continue to be exposed to terrorist financing risks: deposits on accounts represent the easiest way to introduce money into the financial system. In the case of the risk from terrorist financing, the risk exposure is even higher when the origin of funds is legitimate. The use of funds in deposit accounts for terrorist purposes is difficult to detect as low amounts of money are usually used by terrorist groups. When it comes to sending money to conflict zones, the terrorist financing risk is lower in deposits on accounts as perpetrators prefer the use of other products such as money value transfer services or E-money products.

b) risk awareness

The risk awareness of credit and financial institutions is generally good, and the banking sector has put in place guidance to detect the relevant red flags on terrorist financing. However, systems and checks that firms put in place to mitigate the terrorist financing risk are similar to, and often the same as, the checks put in place for anti-money laundering purposes. Supervisors and law enforcement agencies are aware of vulnerabilities to terrorist financing and are proactively engaged with the sector.

[35] See previous footnote.

c) legal framework and checks

Deposits on accounts have been covered by the framework on anti-money laundering (AML) and countering the financing of terrorism (CFT) since the first AML/CFT legislation at EU level in 1991. Checks in place are generally considered as efficient, although sanctions screening is not a substitute for effective CFT checks. Financial sanctions target individuals or groups that are already known to pose a threat, whereas the risk from terrorist financing often emanates from individuals who are not caught by the sanctions regime. This is why risk- based AML/CFT checks, and transaction monitoring in particular, are key to an effective fight against terrorist financing.

Usually, banks do not have access to relevant information that would help them identify terrorist financing risks before they materialise, as such information is often held by law enforcement agencies. Likewise, law enforcement agencies' efforts to disrupt terrorist activities and networks can be hampered in cases where they are unable to obtain information about finance flows that only firms can provide. There are now initiatives at national and supranational levels to test how law enforcement agencies can provide firms with more specific and meaningful information on specific persons of interest, allowing firms to focus their transaction monitoring on these persons.

Conclusions: risk exposure may be considered as quite high, and the sector, despite a good level of awareness, needs to improve the efficiency of checks to mitigate the terrorist financing risk. Engagement with law enforcement agencies is essential in this area. As a result, the level of terrorist financing vulnerability related to deposits on accounts is considered as significant (level 3).

Money laundering

Money laundering vulnerability mainly depends on the effectiveness of monitoring systems to detect suspicious transactions when cash enters bank accounts or transactions linked to cash. Vulnerability is also high when it comes to transfers of funds from high-risk customers.

a) risk exposure

Deposits on account represent the most straightforward way of introducing money from illicit activities into the financial system. There are high volumes of products where, in the case of cash, the origin of funds cannot be always traced. While deposits are a rather common practice for credit and financial institutions, they represent a high number of operations that may involve different kind of customers. Some customers may be high-risk because they are politically exposed or because they are identified as high-risk customers (i.e. some non-resident bank accounts in EU banks).

The extensive use of cash in some sub- sectors and in some Member States is considered by most supervisors to be one of the contributing factors that exposes the sector to money laundering vulnerabilities, particularly where the sector is made up of many retail banks. Supervisors also consider cross- border activities as being exposed to a significant and very significant money laundering risk, particularly in those Member States that are known as international financial centres. Non- resident customers from high- risk

jurisdictions and off- shore companies also contribute to the increased inherent risk in this sector. In some Member States where the domestic deposit base is small to relative to the size of the financial sector, non-resident deposits, especially from bordering non-EU countries, are an attractive source of funding. However, experience of recent years has shown that such deposits, depending on the source jurisdiction and other circumstances, often required reinforced AML controls, which were not in place or not commensurate to the level of risk they presented. Excessive risk taking by credit intuitions resulted in significant exposure of the EU jurisdictions to the flow of funds of potentially suspicious origin from third countries. A recent trend is a steady decrease of the proportion of non-resident deposits in EU jurisdictions – due to both voluntary de-risking by the banking sector as well as public policies of the EU jurisdictions concerned.

b) risk awareness

The risk awareness is generally good, as the sector has in place guidance to detect the relevant red flags on money laundering. While the banking sector has an inherently high exposure to money laundering risks, it also has adequate tools to detect them. This is confirmed by a high levels of reporting. Financial intelligence units and law enforcement agencies are also well aware of the vulnerabilities of the sector and are proactively engaged with it.

For supervisors, while the banking sector is considered inherently risky, as credit institutions are often the first entry point into the overall financial services sector, the concentration of firms rated at very significant risk is relatively small. However, in recent years, scandals in European banks has shown that weaknesses linked to customers from former Soviet republics increase the vulnerability to money laundering.

c) legal framework and checks

Deposits on accounts have been covered by the AML/CFT framework since the first AML/CFT legislation at EU level in 1991. Checks in place are considered as efficient, but it may be necessary to perform thematic supervision to check the effectiveness of the monitoring systems used to detect suspicious cash transactions, especially when legal entities and legal arrangements are involved. Supervisors are also concerned about checks put in place by credit institutions for managing risks associated with customers involving complex off- shore structures; in particular, checks to identify and verify beneficial owners are considered insufficiently robust.

Conclusions: the inherent money laundering risk associated with deposits is appropriately mitigated by credit institutions. However, there are still some concerns about the effectiveness of checks, in particular checks on customers with complex offshore structures and on foreign customers from high-risk jurisdictions. In this context, the level of money laundering vulnerability related to deposits on accounts/retail banking is considered as significant (level 3).

Mitigating measures

For the Commission:

- deep review of the transposition of the 5th Anti-money Laundering Directive (AMLD), focusing on the provisions on beneficial ownership information, including the interconnection of beneficial owner registers at EU level;

- uniform practices in e-identification for the financial sector and introduction of standards to meet customer due diligence obligations with Reg-Tech companies;

- promote cooperation between law enforcement agencies and financial institutions to improve effectiveness of terrorist financing alert systems at supranational level.

For Member States / competent authorities:

· public-private sector cooperation to exchange information related to terrorist financing

· thematic inspections focusing on:

  - assessing the efficiency of monitoring systems for cash transactions and the placing of funds in bank accounts linked to the simultaneous transfer of funds to high-risk non-EU countries.

  - effectiveness of customer due diligence and enhanced customer due diligence for legal entities and legal arrangements.

2. 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 complementary pillars. The first pillar comprises the mutual fund industry, the 'UCITS' funds (€9.7 trillion of assets under management in 2017). The second pillar includes alternative investment funds (the alternative investment fund industry had a net asset value of 4.9 trillion euros at the end of 2017) such as hedge funds (11%), private equity (4%), funds of funds (16%) and real estate funds (11%). Assets managed in EU passed the EUR 15 trillion threshold at the end of 2017. The EU asset management industry serves both retail clients — usually composed of households and high net worth individuals — and institutional clients. Institutional clients comprise, for instance, insurance companies and pension funds, which accounted for 25% and 28% respectively of the total assets managed in EU at end-2016.

Description of the risk scenario

There are several scenarios where perpetrators can commit abuses against investors or financial markets, for instance, through integration of proceeds, such as title of shares to conceal beneficial ownership. Through fraud, or through market abuse (which comprises insider dealing, market manipulation, and unlawful disclosure of inside information, all of which are covered by the scope of the EU Market Abuse Regulation[36] and the EU Criminal Sanctions for Market Abuse Directive[37]), brokerage accounts, investment to justify criminal proceeds as profit, predicate investment fraud, or placement of proceeds using specialised high-return financial services.

General comments

This risk scenario can be seen as linked to the scenario for investment provided by brokers. It has been considered that as far as the money laundering vulnerability is concerned, the level of risk is higher for brokers.

[36] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC Text with EEA relevance; OJ L 173, 12.6.2014, p. 1–61.
[37] Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive); OJ L 173, 12.6.2014, p. 179–189.

Threat

Terrorist financing

The terrorist financing threat related to institutional investment could be significant if large amounts of legitimate funds are invested to finance terrorism, but when it comes to generating small amounts to commit terrorist attacks, the terrorist financing threat is not significant in this product/sector.

Conclusion: the assessment of the terrorist financing threat related to institutional investment through banks is considered as less significant (level 1).

Money laundering

The increasing role of facilitators in money laundering schemes can make the sector more exposed to such threats, although knowledge and technical expertise are needed to carry them out. Criminal organisations could rely on such facilitators to launder the proceeds of illegal activities. Although large amounts of funds can be gathered through this process, it is not easy to access, not financially viable (depending on the quality of investment) and in any case requires knowledge and technical expertise. Therefore, criminal organisations do not favour this kind of risk scenario, while the role of facilitators is essential when creating opaque structures to hide the proceeds of criminal activities.

Nevertheless, a few methods for moving large illicit flows, prepared by highly skilled facilitators, have been identified over the last few years:

- capital market commodity clients conducting over-the-counter future swaps through exchanges, and using illicit funds to settle once expired;
- the simultaneous purchase, transfer and sale of securities across jurisdictions by two seemingly unrelated, but mutually controlled, entities;
- capital market fixed income clients conducting bond trades on behalf of organised criminals, using illegitimate money to purchase bonds and then integrate funds into financial institutions after sale of those bonds.

Conclusions: in this context, the assessment of the money laundering threat related to institutional investment through banks is considered as significant (level 3).

Vulnerability

Terrorist financing

Terrorist financing vulnerability related to institutional investment presents a less significant inherent risk. Risk factors (products, customers, geographies and delivery channels) do not favour the use of this product/sector for terrorist financing purposes. Perpetrators usually do not have the expertise to access the sector, while the low amounts of money used in terrorist attacks made other sectors more attractive for their purposes.

Conclusion: in light of the above, the assessment of the terrorist financing vulnerability related to institutional investment through banks is considered as less significant (level 1).

Money laundering

The assessment of the money laundering vulnerability related to institutional investment — banks made the following findings:

a) risk exposure

The main factor that mitigates the inherent risk money of laundering is the low level of cash-based transactions, despite the fact that the sector is exposed to high-risk customers, including politically exposed persons, while the volume and level of cross-border transactions are high. To have access to the sector, perpetrators need to introduce money through the banking system, and hiding illegal money through opaque structures requires a high degree of expertise. Therefore, banks are a first barrier that mitigates the inherent money laundering risk.

b) risk awareness

Risk awareness in the sector is not high when transactions are performed out of the banking sector. This is because firms usually rely on banks to apply customer due diligence and monitoring when money enters bank accounts.

Supervisors consider the overall risk of the sector moderately significant; however, the risk profile at firm level shows that a significant proportion of firms are classified as a less significant risk. Despite this, most supervisors consider this sector to pose a very significant cross-border risk. Another key risk this sector is exposed to is reconciling the anti-money laundering standards of the home and host Member States where there are branches of a group in different countries.

According to financial intelligence units, the number of suspicious transaction reports is quite low compared to the volume of transactions concerned, due to the sector being more familiar with detecting fraud such as insider trading or market abuse than suspicions of money laundering. At the same time, the financial transactions concerned are more complex and the suspicious ones are probably less easy to detect by obliged entities.

The sector also experiences significant conflict of interest between concerns over money laundering and the need to attract customers, some with a high money laundering risk profile, such as politically exposed persons, customers from high-risk non-EU countries and high-income customers. In that sense, the fact that the service is provided by a broker affects the level of vulnerability to money laundering, rendering it higher than the vulnerability concerning credit institutions.

c) legal framework and checks

Institutional investments through banks are covered by AML/CFT requirements at EU level. 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 relaxed in the implementation of customer due diligence.

Supervisors consider that poor checks are limiting the effectiveness of suspicious transaction reporting and the effectiveness of ongoing monitoring policies and procedures, including transaction monitoring. In contrast, most breaches identified in inspections were considered as minor. The most common finding was poor quality checks on politically exposed persons.

Conclusions: the risk exposure is inherently high due to the nature of the customers and the large amounts linked to the transactions. However, inherent risk is mitigated due to a low level of cash-based transactions and due to bank anti-money laundering checks when investment services are provided by credit institutions. Nevertheless, the use of opaque structures or complex schemes can increase vulnerability if obliged entities do not have the resources to detect and report to financial intelligence units. In light of this, the money laundering vulnerability related to institutional investment provided through banking institutions is considered as moderately significant/significant (level 2/3).

Mitigating measures

For the Commission:

- deep review of the transposition of the 5th AMLD, focusing on the provisions related to beneficial ownership information, including the interconnection of beneficial owner registers at EU level;

- uniform practices in e-identification for the financial sector and introduction of standards to meet customer due diligence obligations with Reg-Tech companies.

For Member States / competent authorities:

- entry into force of Directive 2018/822/EU from 2020, under which intermediaries are required to submit information on reportable cross-border tax arrangements to their national authorities;

- deepen and improve the implementation of beneficial ownership registers and interconnection, as set out in 5th AMLD;

- public-private sector cooperation to exchange information related to terrorist financing;

- thematic inspections to assess:

  - effectiveness of customer due diligence and enhanced customer due diligence as they apply to legal entities and legal arrangements, and how beneficial owner identification requirements are implemented.

3. 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 complementary pillars. The first pillar comprises the mutual fund industry, the 'UCITS' funds (€9.7 trillion of assets under management in 2017). The second pillar includes alternative investment funds (the alternative investment fund industry had a net asset value of 4.9 trillion euros at the end of 2017) such as hedge funds (11%), private equity (4%), funds of funds (16%) and real estate funds (11%). Assets managed in EU passed the EUR 15 trillion threshold at the end of 2017. The EU asset management industry serves both retail clients — usually composed of households and high net worth individuals — and institutional clients. Institutional clients comprise, for instance, insurance companies and pension funds, which accounted for 25% and 28% respectively of the total assets managed in EU at end-2016.

Description of the risk scenario

There are several scenarios where perpetrators can commit abuses against investors or financial markets, for instance, through integration of proceeds, such as title of shares to conceal beneficial ownership. Through fraud, or through market abuse (which comprises insider dealing, market manipulation, and unlawful disclosure of inside information, all of which are covered by the scope of the EU Market Abuse Regulation and the EU Criminal Sanctions for Market Abuse Directive), brokerage accounts, investment to justify criminal proceeds as profit, predicate investment fraud, or placement of proceeds using specialised high-return financial services.

General comments

This risk scenario can be seen as linked to the scenario for investment provided by brokers. It has been considered that as far as the money laundering vulnerability is concerned, the level of risk is higher for brokers.

Threat

Terrorist financing

The terrorist financing threat related to institutional investment — brokers (securities, asset management, and investment) could be relevant if large amounts of legitimate funds are invested for financing terrorism, but when it comes to small amounts of funds to commit terrorist attacks, the threat is not significant in this product/sector.

Conclusion: the assessment of the terrorist financing threat related to institutional investment through brokers is considered as less significant (level 1).

Money laundering

The increasing role of facilitators in money laundering schemes can make the sector more exposed to such threats, although knowledge and technical expertise are needed to carry them out. Criminal organisations could rely on such facilitators to launder the proceeds of illegal activities. Although large amounts of funds can be gathered through this process, it is not easy to access, not financially viable (depending on the quality of investment) and in any case, it requires knowledge and technical expertise. Therefore, criminal organisations do not favour this kind of risk scenario, while the role of facilitators is essential when creating opaque structures to hide the proceeds of criminal activities.

Nevertheless, a few methods for moving large illicit flows, prepared by highly skilled facilitators, have been identified over the last few years:

- capital market commodity clients conducting over-the-counter future swaps through exchanges, and using illicit funds to settle once expired;
- the simultaneous purchase, transfer, and sale of securities across jurisdictions by two seemingly unrelated, but mutually controlled, entities;
- capital market fixed income clients conducting bond trades on behalf of organised criminals, using illegitimate money to purchase bonds and then integrate funds into financial institutions after sale of those bonds.

Conclusions: in this context, the assessment of the money laundering threat related to institutional investment through brokers is considered as significant (level 3).

Vulnerability

Terrorist financing

Terrorist financing vulnerability related to institutional investment — brokers (securities, asset management, and investment) presents a low significant inherent risk. The different risk factors, products, customers, geographies and delivery channels in the sector mean that its use for terrorist financing purposes is not favoured. In that sense, perpetrators usually do not have the expertise to access the sector, while the low amounts of money used in terrorist attacks made other sectors more attractive for their purposes.

Conclusion: in light of the above, the assessment of the terrorist financing vulnerability related to institutional investment through brokers is considered as less significant (level 1).

Money laundering

The assessment of the money laundering vulnerability related to institutional investment — brokers (securities, asset management, and investment) made the following findings:

a) risk exposure

The main factor that mitigates the inherent risk of money laundering is the low level of cash-based transactions, despite the fact that the sector is exposed to high-risk customers, including politically exposed persons, while the volume and level of cross-border transactions are high. To have access to the sector, perpetrators need to introduce money through the banking system, and hiding illegal money through opaque structures requires a high degree of expertise. Therefore, banks are a first barrier that mitigates the inherent money laundering risk.

b) risk awareness

Risk awareness in the sector is not high when transactions are performed out of the banking sector. This is because firms usually rely on banks to apply customer due diligence and monitoring when money comes from bank accounts.

Supervisors consider the overall risk of the sector moderately significant; however, the risk profile at firm level shows that a significant proportion of firms are classified as a less significant risk. Despite this, most supervisors consider this sector to pose a very significant cross-border risk. Another key risk this sector is exposed to is reconciling the AML standards of the home and host Member States where there are branches of a group in different countries.

According to financial intelligence units, the number of suspicious transaction reports is quite low compared to the volume of transactions concerned, due to the sector being more familiar with detecting fraud such as insider trading or market abuse than suspicions of money laundering. At the same time, the financial transactions concerned are more complex and the suspicious ones are probably less easy to detect by obliged entities.

The sector also experiences significant conflict of interest between concerns over money laundering and the need to attract customers, some with a high money laundering risk profile, such as politically exposed persons, customers from high-risk non-EU countries and high-income customers. In that sense, the fact that the service is provided by a broker affects the level of vulnerability to money laundering, rendering it higher than the vulnerability concerning credit institutions.

c) legal framework and checks

Institutional investments through brokers 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 be more relaxed in the implementation of customer due diligence.

Supervisors consider poor checks are limiting the effectiveness of suspicious transaction reporting and the effectiveness of ongoing monitoring policies and procedures, including transaction monitoring. In contrast, most breaches identified in inspections were considered as minor. The most common finding was the poor quality checks on politically exposed persons.

Conclusions: the risk exposure is inherently high due to the nature of the customers and the large amounts linked to the transactions. However, inherent risk is mitigated due to a low level of cash-based transactions. When investment services are provided by brokers, money laundering vulnerability is higher than when those services are provided by banks. Lack of resources to apply robust customer due diligence procedures and some conflict of interest over attracting customers with a high-risk money laundering profile can increase vulnerability. In this context, the money laundering vulnerability related to institutional investment provided through brokers is considered as significant (level 3).

Mitigating measures

For the Commission:

- deep review of the transposition of the 5th AMLD, focusing on the provisions related to beneficial ownership information, including the interconnection of beneficial owner registers at EU level;

- entry into force of Directive 2018/822/EU from 2020, under which intermediaries are required to submit information on reportable cross-border tax arrangements to their national authorities

- uniform practices in e-identification for the financial sector and introduction of standards to meet customer due diligence obligations with Reg-Tech companies.

For the European supervisory authorities:

- Guidelines on best supervisory practices to the investment sector. Define the main money laundering risk scenarios and products, alongside the most effective ways to conduct on-site and off-site inspections.

For Member States / competent authorities:

- deepen and improve the implementation of beneficial ownership registers and interconnection, as set out in 5th AMLD;

- public-private sector cooperation to exchange information related to terrorist financing;

    - thematic inspections to assess:

    - effectiveness of customer due diligence and enhanced customer due diligence as they apply to legal entities and legal arrangements, and how beneficial owner identification requirements are implemented.

4. 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 the legal economy using company accounts with multiple signatories.

Threat

Terrorist financing

Corporate banking can provide large amounts of legitimate funds to finance terrorist activities or send money to conflict zones. However, that risk scenario is not probable as small amounts of money are used in terrorist attacks and as there are other products/sectors less traceable to send money to risky areas. Perpetrators do not prefer these kind of products to finance terrorist activities, so the terrorist financing threat is not significant in this product/sector.

Conclusion: the assessment of the terrorist financing threat related to corporate banking is considered as less significant (level 1).

Money laundering

The assessment of the money laundering threat related to corporate banking shows that this risk scenario has been recurrently used for such schemes. Using corporate banking for money laundering requires more sophistication than the retail financial sector, but depending on the financial service concerned, the level of sophistication required may be lower: for instance, personal documentation is required only if there is demand for a loan. Nevertheless, given the level of sophistication that corporate banking operations require, using them for money laundering would require the complicity of financial/legal intermediaries who need to be paid for their 'services'. This is parameter may have an impact on the intent component.

Law enforcement agencies have evidence of professional money launderers acting as intermediaries for other organised crime groups that set up bank accounts for front or shell companies. Those corporate bank accounts are used for fake trade transactions, back-to-back loans with other corporate entities and real estate investments.

Conclusions: this method is used by organised crime groups, with an increasing role for intermediaries. In the view of law enforcement agencies, this method requires only moderate levels of knowledge and expertise. In this context, the money laundering threat related to corporate banking is considered as significant (level 3).

Vulnerability

Terrorist financing

The inherent risk of terrorist financing vulnerability in the corporate banking sector is of low significance. The different risk factors, products, customers, geographies and delivery channels in the sector mean that its use for terrorist financing purposes is not favoured. Perpetrators usually do not have the expertise to access the sector, while the low amounts of money used in terrorist attacks made other sectors more attractive for their purposes.

Conclusion: in light of this, the assessment of the terrorist financing vulnerability related to institutional investment through banks is considered as less significant (level 1).

Money laundering

The assessment of the money laundering vulnerability related to corporate banking made the following findings:

a) risk exposure

The inherent risk is potentially high due to the nature of customers and due to more complex transactions than in retail banking being involved. The identification of the beneficial owner of some firms is one of the main vulnerabilities of this product. Some trade-base transactions linked to corporate bank accounts can increase the money laundering risk, especially when high-risk jurisdictions are involved. The risk linked to forged documentation also affects the level of risk exposure, while the increasing role of intermediaries and facilitators working for organised crime groups can also affect the inherent risk of these products. Some cash-based transactions can be settled using these products when firms involved in corporate banking products are cash-intensive businesses.

Moreover, the inherent risk in these banking products can also be increased by the use of new technologies and non-face-to-face business relationships.

For anti-money laundering supervisors, differences in the make- up and nature of Member States' credit institution sectors are reflected in inherent risk ratings, which range from 'significant' and 'very significant' to 'moderately significant' and even 'less significant'. On the other hand, most supervisors regard the extensive use of cash in some sub- sectors and in some Member States as one of the contributing factors exposing the sector to money laundering vulnerabilities, particularly where the sector is made up of many retail banks. Supervisors also consider cross- border activities to be exposed to a significant risk and very significant risk of money laundering, particularly in those Member States known as international financial centres. Non- resident customers from high- risk jurisdictions and off- shore companies also contribute to the increased inherent risk in this sector.

a) risk awareness

Sector awareness of risk is high, and the sector has developed tools to trigger appropriate red flags. Usually red flags are triggered in response to high-risk customers, high-risk jurisdictions and the existence of cross-border transactions. Financial intelligence units have confirmed this element, mentioning that a high number of suspicious transaction reports have been received on this matter. However, sector complaint about lack of feedback from FIUs. That fact is limiting the sector's ability to improve its monitoring systems.

In most Member States, AML supervisors provide guidelines to help credit institutions detect potentially suspicious corporate banking transactions.

b) legal framework and checks

Corporate banking is covered by AML/CFT requirements at EU level. This framework is considered as satisfactory as the framework covering other financial activities undertaken by credit institutions.

Most supervisors assessed the checks put in place by credit institutions to mitigate money laundering risks as 'good' or 'very good' overall. Despite this, they assess the effectiveness of these policies and procedures, particularly those related to ongoing monitoring of transactions and suspicious transactions reporting, as poor or very poor.

Conclusions: corporate banking presents some vulnerability due to risk factors associated with customers. However, the legal framework in place is considered as being adapted to these vulnerabilities, while credit institutions involved in corporate banking activities are aware of the money laundering risks and are equipped to address them. In this context, the level of money laundering vulnerability related to corporate banking is considered as moderately significant/significant (level 2/3).

Mitigating measures

For the Commission:

- deep review of the transposition of the 5th AMLD, focusing on the provisions related to beneficial ownership information, including the interconnection of beneficial owner registers at EU level;
- uniform practices in e-identification for the financial sector and introduction of standards to meet customer due diligence obligations with Reg-Tech companies;
- entry into force of Directive 2018/822/EU from 2020, under which intermediaries are required to submit information on reportable cross-border tax arrangements to their national authorities.

For the European supervisory authorities (ESAs):

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

For Member States / competent authorities:

- Authorities should provide training sessions and guidance on risk factors, with specific focus on non-face-to-face business relationships, offshore professional intermediaries, customers or jurisdictions, and on complex/shell structures.
- Thematic inspections to assess:
    - effectiveness of customer due diligence and enhanced customer due diligence as they apply to legal entities and legal arrangements, and how beneficial owner identification requirements are implemented.

5. Private banking sector

Product
Deposits on accounts

Sector
Credit institutions — Private banking and wealth management

Description of the risk scenario
Private banking is a service provided by credit institutions and investment firms to high net worth individuals, their families and corporate entities. In general, these services are tailored for each customer by combining multiple banking and other financial services in one package. For example, private banking services may include a mix of banking services (current accounts, mortgages and foreign exchange), investment management and advice, fiduciary services, safe custody, insurance, accounting, tax and estate planning and associated services, such as legal support.

Perpetrators are using private banking and wealth management to invest in shares for integration of criminal proceeds. Given the combination of sophisticated financial products and services, and a wealthy customer base, sometimes PEPs, with often complex ownership structures, the sector can be abused also for tax evasion.

General comments

For this risk scenario, financial services concern high-value investments and not investments by individuals in retail services.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to private banking (wealth management) has not been considered as relevant. Therefore the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering 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 also requires some level of expertise, which makes it less easy to access and not very attractive (not financially viable). In private banking, the service is quite 'high cost' (need for sufficient funds to access the services) and the business relationship less easy to establish. However, some groups can use facilitators to obtain access to private banking services through frontmen or legal persons.

Conclusions: based on the above, the money laundering threat related to private banking is considered as significant/very significant (level 3/4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to private banking (wealth management) has not been considered as relevant. In this context, the terrorist financing vulnerability is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering vulnerability related to private banking (wealth management) made the following findings:

a) risk exposure

The combination of sophisticated financial products and services, and a wealthy customer base (sometimes politically exposed persons) with often complex ownership structures make this sector highly vulnerable for money laundering purposes. Some of the products and services offered are also considered to present money laundering vulnerabilities, particularly those linked to tax compliance and planning. 'Aggressive' tax planning appears to be one such type of service. Furthermore, the sector presents a higher geographical risk due to the establishment of branches in some non-EU countries that do not have necessarily equivalent AML/CFT regimes to the EU's AML/CFT framework.

b) risk awareness

According to financial intelligence units, private banking is characterised by a very low (almost inexistent) level of suspicious transaction reporting. As for investment services, institutions sometimes face conflict between their commercial objectives and the need to fight against money laundering. The competition component is not negligible. However, for private banking the risk assessment is not always precise enough to ensure that the sector is aware of the risks it faces, in particular risks linked to fraud and tax evasion. Supervisors consider that firms in this sector do not adequately mitigate the risk of the sector being abused for tax evasion purposes.

c) legal framework and checks

Private banking is covered by AML/CFT requirements at EU level. Most competent authorities that have inspected providers of private banking services have assessed the level of checks as 'inadequate' for customer due diligence (verification of customer's identity, information about the origin of funds, verification of beneficial ownership — specifically with legal persons), monitoring transactions, and compliance function. They explain this weakness by: (i) the fact that the quality of the checks depends on the financial culture of a country; and (ii) that the understanding of the risks posed by this sector is not the same from one Member State to another.

Conclusions: High inherent risk due to the large amounts involved, high-risk customers (politically exposed persons) and potentially high-risk jurisdictions. Concerns about the sector's risk awareness due to the competition between providers to attract high-risk customers, while the results of thematic inspections that have shown inadequate checks in certain areas. Moreover, the level of suspicious transaction reporting is low. In this context, the level of money laundering vulnerability related to private banking is considered as significant/very significant (level 3/4).

Mitigating measures

For the Commission:

- deep review of the transposition of the 5th AMLD, focusing on the provisions related to beneficial ownership information, including the interconnection of beneficial owner registers at EU level;
- uniform practices in e-identification for the financial sector and introduction of standards to meet customer due diligence obligations with Reg-Tech companies;
- entry into force of Directive 2018/822/EU from 2020, under which intermediaries are required to submit information on reportable cross-border tax arrangements to their national authorities.

For the European supervisory authorities:

- European supervisory authorities to provide training sessions to competent authorities, focusing on a common approach to inspections and the main risk areas.

For Member States / competent authorities:

- Thematic inspections to assess:
  - effectiveness of customer due diligence and enhanced customer due diligence as they apply to legal entities and legal arrangements and how beneficial owner identification requirements are implemented.
- Risks associated with this sector should be clearly set out in the competent authorities' money laundering/terrorist financing risk assessment. Competent authorities should issue guidance on best practices and provide training to the sector.
- Competent authorities should ensure that systems and checks are put in place to reduce firms' ability to design or recommend products and services that help their customers commit tax crimes.

6. Crowdfunding

Product
Crowdfunding

Sector
Crowdfunding platforms

General description of the sector and related product/activity concerned

Crowdfunding is 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 type of fundraising activities varies greatly across the different crowdfunding models. There is also variation in the motivation and type of participants, as well as the resulting relationship between investors/lenders and fund seekers/borrowers. There are different models of crowdfunding platforms and any categorisation is provisional as the market develops and integrates new technologies into service provision. The five main categories of crowdfunding platforms are:

- 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 in which 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.

There are a number of platforms that combine different models or which run a model that cannot be immediately classified under these five categories ('hybrid models of crowdfunding'). However, they are usually of a much smaller scale than the main ones.

Another relevant classification of crowdfunding platforms depends on whether are authorised or not:

- Regulated crowdfunding platforms, which fall under the scope of an ongoing financial services legislative initiative (i.e. investment-based and lending-based platforms) and are thus accordingly authorised.
- Unregulated crowdfunding platforms that fall outside the scope of the financial services legislation (i.e. donation, reward-based, consumer lending crowdfunding). This also includes websites, i.e. social media platforms, messaging apps or blogs with a potentially wide outreach, which may enable their users to make a public call for collection of funds, but where the platform itself does not facilitate this process.

It should also be taken into account that whilst platforms introduce and connect the relevant parties, the actual monetary transactions are normally carried out by authorised providers of payment services, which are under the scope of AMLD legislation. A further distinction should therefore be made between regulated crowdfunding, where transactions occur through authorised payment providers (i.e. by integration with PayPal or by referencing personal bank accounts) on regulated crowdfunding platforms that are subject to additional disclosure requirements, and unregulated crowdfunding, which are not currently under the scope of financial services legislation. In the unregulated area, in particular, payments may also take place via less transparent means, i.e. crypto-assets or pre-paid sim card tokens.

The European alternative finance market as a whole raised a total of €10.44 billion in 2017, up 36% on the previous year. The market remains heavily dominated by the UK, which had a market share of 68% with €7.07 billion in 2016, down from 75% in the previous year. The rest of the European market raised a total of €3.37 billion and grew at a rate of 63% in that year. This makes crowdfunding the most important sub-market of the alternative finance sector. Excluding the UK, the countries with the largest total market volumes in 2016 were France, Germany, the Netherlands, Italy and Finland.

Examining the market share in more detail, peer-to-peer consumer lending has the largest market share with 41%, followed by invoice trading (16%), peer-to-peer business lending (14%), real estate crowdfunding (8%) and equity-based crowdfunding (6%).

Description of the risk scenario

Perpetrators can create platforms to collect/accumulate funds and transfer them abroad for money laundering purposes or to finance terrorist attacks. This can be done by creating a regulated crowdfunding platform directly linked to a financial institution[38] or by setting up a platform outside a regulated environment and not linked to a financial institution where payments can be in virtual currency, e-money cards, etc... Non authorised crowdfunding platforms can be set up under fictitious projects to collect funds, which are then withdrawn within the EU or transferred abroad. This method could be used either to collect funds from legitimate sources to fund terrorism or to collect illicit funds from criminal activities using anonymous products.

[38] Linked to a bank account, or with a bank partnership.

Misuse of social media ('crowdsourcing') is 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 analysed further here.

Threat

Terrorist financing

Terrorist groups may have the intent to use the crowdfunding techniques to collect funds. Overall, there have been few cases relating to (unregulated) donation platforms where these techniques have been used; where they have, it has usually been to raise smaller amounts. In addition, suspicious activities are somewhat easier to detect and may deter terrorist groups from using this method, as it is not the most secure option. However, if perpetrators are more methodical in their planning, this could enable them to set up collection platforms with scope for more anonymous operations (use of strawmen or relatives), thus making this method more attractive. Law enforcement agencies have detected some cases of crowdfunding calls for donation, citing 'support for widows, martyrs, religious groups' in an attempt to avoid clear a linkage with terrorist financing. The value of the donations are low ($10, 20, 50, with most amounts in US dollars). The difficulty for law enforcement agencies is identifying the end recipient and the use of the donations (proof of terrorist financing).

Conclusions: Law enforcement agencies have evidence of terrorist groups using unregulated donation crowdfunding platforms. However, it is not financially viable to raise or channel large amounts this way. Also, it may be rather insecure compared to other types of services, or it requires more planning to hide the illicit intent. In this context, the terrorist financing threat related to crowdfunding is considered as moderately significant (level 2).

Money laundering

The assessment of the money laundering threat related to crowdfunding shows that there is little to no evidence or indicators that criminals have used it to actually launder the proceeds of crime. There are however situations where a company has been set up to be used for crowdfunding criminal activities, but this requires some expertise and can be costly. One case identified concerned a complex Ponzi scheme using scam and fake projects. This suggests that this scenario may be difficult to access and requires having access to payment processes. This would mean that the use of criminal intermediaries could make the sector more attractive for money laundering purposes. However, law enforcement agencies consider that the sector is still used more for scam fundraising and fraud rather than to launder illicit funds.

Conclusions: criminals may have vague intentions to exploit this method, which is not necessarily attractive and may be costly. In any case, the method requires some expertise to be profitable. There is little evidence that it has been used, although the role of intermediaries is not negligible. In this context, the level of the money

laundering threat related to crowdfunding is considered as moderately significant (level 2)

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to crowdfunding shows that the sector cannot be assessed in isolation.

a) risk exposure

The level of risk exposure varies depending on depending on whether the crowdfunding platform is supervised as a provider of financial services or is left unregulated (private initiatives on the internet). Likewise, the terrorist financing risk also depends on the type of platform. Unregulated donation-based crowdfunding platforms present a higher inherent risk of misuse for terrorist financing purposes as these platforms are outside the scope of financial institutions and of prudential and anti-money laundering supervisors. The inherent risk of crowdfunding is higher if crowdfunding platforms allow use of virtual currencies or (anonymous) electronic money. The inherent risk is also higher if perpetrators set up donation-based crowdfunding platforms allowing the use of strawmen, relatives or individuals out of the scope of sanction lists.

b) risk awareness

Even when a crowdfunding platform is regulated as a financial service provider, there may be a lack of knowledge about the sources of funds and the purpose. When provided through unregulated platforms, crowdfunding services are outside the scope of any AML/CFT monitoring. Competent authorities, including at EU level, are aware that terrorist financing risks exist, but the risk assessment is still incomplete in most Member States. It should, however, be stressed that where these platforms are included in the list of obliged entities, financial intelligence units will receive suspicious transaction reports.

c) legal framework and checks

As far as the EU AML/CFT framework is concerned, it is not generally applicable to crowdfunding platforms as such but is applicable to specific types of crowdfunding services depending on the business model. Hence, there is no cross-cutting framework setting AML/CFT obligations for those services.

Crowdfunding platforms have bespoke regulation in some Member States, mainly for securities and lending, which means that donation platforms are not covered by the AML/CFT obligations. Some Member States have included crowdfunding platforms in their legislation transposing the Payment Services Directive II. However, competent authorities consider that checks and supervisory actions are weak, particularly as many platforms are not established physically in the territory where they operate, which hinders the efficiency of checks. Where credit and financial institutions are involved, the effectiveness of obliged entities' checks is lower as the obliged entities can rely only on more limited information to monitor transactions and apply red flags.

Conclusions: the sector is not homogeneous and the interdependency with other sectors can impact the level of vulnerabilities. Checks in place are not harmonised because there is no cross-cutting framework dealing with this issue, although the new regulation on European crowdfunding business providers will improve this framework. There are some concerns about the risk awareness of the sector. In this context, the level of terrorist financing vulnerability related to crowdfunding is considered as moderately significant (level 2)

Money laundering

The assessment of the money laundering vulnerability related to crowdfunding shows similar vulnerability assessment as for terrorist financing.

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, the use of virtual currencies may increase the inherent money laundering risk. Depending on the type of platform, services may facilitate anonymous transactions. On lending and securities platforms, it is possible to raise larger amounts, making the inherent risk of money laundering higher than for donation platforms. However these crowdfunding platforms would normally be regulated, thus complying with disclosure requirements, and partner with payment or credit institutions in order to carry out payment transactions.

b) risk awareness

The infiltration of such platforms by criminal organisations should also be considered an additional vulnerability factor. Some law enforcement agencies and financial intelligence units tend to regard crowdfunding as 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 unregulated entities, crowdfunding services are outside the scope of any AML/CFT monitoring. Competent authorities, including at EU level, are aware that money laundering risks exist but some of them consider this sector as low risk and are not considering including crowdfunding platforms as obliged entities. It should, however, be stressed that where these platforms are included in the list of obliged entities, financial intelligence units will receive suspicious transaction reports.

c) legal framework and checks

As far as the EU AML/CFT framework is concerned, it is not generally applicable to crowdfunding platforms as such but is applicable to specific types of crowdfunding services depending on the business model. Hence, there is no cross-cutting framework setting AML/CFT obligations for those services.

Specific types of crowdfunding services will in most cases be covered by AML/CFT obligations, depending on the business model (e.g. investment-based and lending-based crowdfunding). Some Member States have included crowdfunding platforms in their legislation transposing Markets in Financial Instruments Directive II and the Payment

Services Directive II. However, at this stage, not all Member States are considering including crowdfunding platforms as obliged entities.

Even when crowdfunding platforms are considered obliged entities, competent authorities consider that checks and supervisory actions are weak, particularly as many platforms are not established physically in the territory where they operate, which hinders the efficiency of checks. Where credit and financial institutions are involved, the intensity of obliged entities' checks may be lower if the obliged entities can rely only on more limited information to monitor transactions and apply red flags.

Conclusions: the risk exposure is rather limited, although large sums may be involved in some specific crowdfunding business models. The checks in place are not harmonised because there is no cross-cutting framework dealing with this issue. When regulated, these platforms are well aware of their risks and the level of reporting is good. The checks in place are still sometimes weak, especially when obliged entities rely on limited information to carry out checks. The new regulation on European crowdfunding business providers will improve this framework. In this context, the level of money laundering vulnerability is considered as moderately significant (level 2).

Mitigating measures

For Member States / competent authorities:

- When applying Article 4 of the 5th AML Directive extending the scope of obliged entities, Member States should consider the need to define unregulated crowdfunding platforms as obliged entities subject to AML/CFT requirements.

7. 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 terrorist financing threat related to currency exchange shows that this modus operandi is exploited by terrorist groups, especially by foreign terrorist fighters. The EUR/USD conversion is particularly attractive for these groups. Bringing currency into conflict zones is one of the main ways of financing the movement of foreign terrorist fighters. From a technical point of view, the conversion of funds does not require specific planning, knowledge or expertise and is quite easy to access. Although it does not consist in raising or transferring funds, it is a necessary step for moving physically 'clean' currency (most of the time in cash). Terrorist groups may consider that currency exchange is as attractive as collecting or transferring 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 already been used. In this context, the level of terrorist financing threat related to currency exchange is considered as significant (level 3).

Money laundering

The assessment of the money laundering 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 prevalent in offices operating in airport and tourist areas. High volumes of money can be easily converted, making it easy for these criminal organisations to access to 'clean' currency. As with terrorist financing, currency exchange does not require specific planning or expertise for money laundering purposes. However, the volume of suspicious transactions is currently difficult to assess.

Conclusions: although the volume of cases is difficult to assess by law enforcement agencies, the indicators show that criminal organisations may use currency exchange to launder proceeds of crime. This scenario does not require specific planning or expertise and has already been used. In this context, the level of the

money laundering threat related to currency exchange is considered as significant (level 3).

Vulnerability

Terrorist financing

Vulnerability in currency exchange is linked to the transfer of funds. There are two different ways to perform the transactions:

- use of cash to exchange and transfer the funds to a specified bank or payment account;
- use of the internet to perform the currency exchange and transfer the funds to a bank account or payment account.

a) risk exposure

The fact that most of the transactions are in cash increases the sector's vulnerability. Moreover, potential transactions linked to terrorist financing usually involve small amounts of cash that are more difficult to detect by currency exchange offices.

b) risk awareness

In some risk scenarios, money value transfer services (MVTS) providers are associated with currency exchange offices or even operate from the same premises. In such cases, alert systems and red flags applied by MVTS providers to detect terrorist financing-linked transactions are applied to the previous currency exchange transaction. The negative effect is that currency exchange offices rely on MVTS providers' terrorist financing checks. The currency exchange office itself is not in a position to trace the whole transaction, detect potentially suspicious transactions and have a complete business relationship with their customers.

Risk awareness in the sector is high, especially when currency exchange offices are close to MVTS, but the level of suspicious transaction reporting remains low except in specific cases such as USD conversion requested from high-risk non-EU countries (e.g. Syria).

c) legal framework and checks

Currency exchange offices are covered by the AML/CFT framework at EU level. Supervisors consider that checks relating to the effectiveness of suspicious transaction reporting are in general poor or very poor, similar to checks related to customer identification and verification. In that sense, new technological developments may become an important mitigating force for this sector with the increase of online payments. Supervisory activities have been mostly limited to off-site inspections, with some thematic inspections carried out in response to identified concrete risks. When some jurisdictions apply thresholds for occasional transactions, vulnerability is higher, especially for terrorism financing risks, where low amounts are the norm.

Conclusions: Controls in the sector are not very effective and rely on associated sectors such as MVTS providers and banks. Thresholds for occasional transactions can significantly affect the monitoring systems and customer due diligence requirements, increasing terrorist financing vulnerability. In this context, the level of terrorist financing vulnerability related to currency exchange is considered as significant (level 3).

Money laundering

The assessment of the money laundering vulnerability related to currency exchange made the following findings:

a) risk exposure

The fact that most transactions are in cash affects vulnerability; that effect is more pronounced when the customer uses large denomination notes, which are not well monitored. Other factors that increase the sectoral risk are the use of these services by politically exposed persons or the currency exchange offices being located in border zones. The main risk factor is the infiltration of currency exchange offices or agencies by criminal organisations. Inherent risk increases if firms have inadequate tools to detect potentially bad currency exchange agents.

b) risk awareness

In some risk scenarios, MVTS providers are associated with currency exchange offices, or even operate out of the same premises. In such cases, alert systems and red flags applied by MVTS providers to detect money laundering-linked transactions are applied to the previous currency exchange transaction. The negative effect is that currency exchange offices rely on MVTS providers' money laundering checks. For anti-money laundering purposes, the level of reporting is uneven from one Member State to another, and does not necessarily consist in suspicious transaction reports (mostly currency transaction reports).

Supervisors' assessments of the inherent risk for currency exchange sector are divergent, ranging from very significant to less significant. The core current risks identified include: the anonymity of transactions, proximity to border regions and itinerant communities (migrants, cross-border workers, asylum seekers, tourism), and the prevalence of cash transactions. Different competent authorities have identified these as the source of greatest concern.

c) legal framework and checks

Currency exchange offices are covered by the AML/CFT framework at EU level. Supervisors do not consider the currency exchange sector as high-risk in general; according to this assessment, resources to supervise this sector are lower than other sectors. Additionally, many competent authorities cited as ongoing risk factors poor internal checks, a lack of awareness of the relevant regulatory context and poor reporting practices on suspicious activity, despite checks being implemented.

Another factor that hinders proper checks in currency exchange offices is the threshold that can be set out in different countries to apply customer due diligence obligations only for occasional transactions; in any case, most Member States apply thresholds lower than €15,000.

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

Mitigating measures

For Member States / competent authorities

- Competent authorities should conduct a number of on-site thematic inspections focusing on risks posed by agents. The scope of these thematic inspections should include checking that MVTS firms have a comprehensive agent oversight function including efficient monitoring systems, on-site reviews and training.
- Member States should eliminate thresholds for applying customer due diligence to occasional transactions in currency exchange sector in order to improve monitoring of suspicious transactions.

8. 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. E-money can for example be stored on cards, on mobile devices, and 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.

E-money typology

A first classification of e-money products depends on the technology used to store the monetary value: products can be hardware-based or software-based.

For hardware-based products, the purchasing power resides in a physical device, such as a chip card, with hardware-based security features. Monetary values are typically transferred by means of device readers that do not need real-time network connectivity to a remote server.

Software-based products have specialised software that functions on common devices such as computers or tablets. To enable the transfer of monetary values, the device typically needs to establish an online connection with a remote server that controls the use of the purchasing power. Schemes mixing both hardware and software-based features also exist.

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. by a company in the case of business-to-business cards or by a merchant in multi merchant loyalty schemes).

E-money products can be reloaded (to add more value after the initial issuing of e-money by the issuer) or not.

How e-money products are classified depends on whether the product is multifunctional or is linked to a platform. Both types can be used online, but the latter only allows purchases in a single platform and does not allow peer-to-peer transfers. In both cases, a bank account is needed for loading the e-money products. Another category includes prepaid cards or vouchers with customer due diligence exemptions: these products can be used online or offline and can be purchased by cash.

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 are not issued on receipt of funds.

Description of the sector

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 because only euro area 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.

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 €73 billion corresponding to e-money payment transactions with e-money issued by EU resident payment service providers. This €73 billion includes €57 billion in Luxembourg (PayPal, Amazon) and 13 billion in Italy. The number of transactions was 2.09 billion (including 1.5 billion in Luxembourg and some 300 million in Italy). 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 €35. E-money payments represented 3% of the total number of electronic payment transactions in the euro area (EU-18). In the five-year period from 2010-2014, the number of e-money transactions in the EU increased 2 times, and their value 2.5 times.

On the basis of the ECB statistics, the prepaid instrument market in 2014 would have represented €19.3 billion, out of which 13 billion were attributable to Italian 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 office giro institutions are entitled under national law to issue electronic money. E-money can also be issued by the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities. Member States or their regional or local authorities when acting in their public capacity can also issue electronic money.

The majority of e-money issuers are based in the UK and Belgium, as well as in CZ, DK, LV and NL.

As regards the different business models, 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 e-money issuer, enabling issuer to carry out payment services activities (except for issuing e-money) in another Member State without establishing a branch there.

In practice, this distinction appears to be used by the consulted e-money issuers primarily in the context of cross-border provision of e-money services, with selected issuers using 'distribution partners' in order to operate in other Member States[39].

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 using fake or stolen identities, or using strawmen or nominees etc.). Nevertheless, the latter option is costly and it is an easier option for perpetrators to deal with intermediaries in the delivery channel.

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. Only when money stored in cards is used do e-money issuers have the chance to trace or monitor transactions

[39] Opinion of the European Banking Authority on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD) https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+.pdf

Threat

Terrorist financing

E-money products present some advantages over cash when it comes to making online payments, and the use of these products does not require great expertise. Taking into account the low amounts of money needed for terrorist attacks, it can sometimes be easier to pay for some products or services (hotels, car rentals) using e-money products than by cash, even if perpetrators have to pass customer due diligence measures because payments are above the thresholds. On the other hand, e-money products are more traceable than cash.

When perpetrators send money to conflict zones e-money products can be safer to carry out, but using them as a means of payment in those countries can be more complicated than using cash.

Law enforcement agencies have gathered evidence that e-money loaded onto prepaid cards has been used to finance terrorist activities, in particular to help terrorists commit attacks (e.g. hotel or car rentals). However, the threat from using prepaid cards or e-money products for this purpose is independent of the need to get through customer due diligence measures to gain access to e-money products.

In summary, e-money products have some advantages for terrorist financers in comparison with cash. While such products allow for more discrete payments than cash, they bring with them disadvantages when using e-money products in conflict zones or avoiding traceability of the payments. The level of threat is independent of the thresholds for applying customer due diligence if perpetrators are not included in sanction lists.

Conclusions: e-money, specifically in pre-paid cards, is attractive for terrorist groups because it is a simple way to finance their activities. Given the low amounts of money used, it is a discrete way to make payments. However, cash is still a preferred way to send money to conflict zones or to avoid traceability. Law enforcement agencies have evidence that this modus operandi has been used, but the threat is independent of the thresholds for apply customer due diligence. In this context, the level of terrorist financing threat related to e money is considered as significant (level 3).

Money laundering

The assessment of the money laundering threat is linked to some cash-based products that can be used by criminal organisations, including non-EU ones, through distributors of these products. E-money products have some advantages over cash when it comes to moving that money outside the EU or to different Member States. Nevertheless, cash remains a preferred option for these groups.

Financial intelligence units have detected multiples cases of misuse of e-money (tax fraud, drug trafficking, prostitution) through the purchase of multiple prepaid cards. Law

enforcement agencies have found cases where the proceeds of drug trafficking were laundered by prepaid cards. Prepaid cards may enable large amounts to be moved about easily. However, since the use of frontmen is costly when circumventing customer due diligence thresholds and laundering large amounts of money, it easier to use agents involved in the delivery channel of e-money products.

Conclusions: Unlike in the case of terrorist financing, e money is attractive for criminal organisations due to the large amounts of money used, especially when loaded onto prepaid cards or vouchers with customer due diligence exemptions, which can be used online or offline and can be purchased by cash. However due to the lower thresholds, some connection is needed with e-money issuers' agents or distributors in their delivery channels. Nevertheless, criminal organisations prefer to use cash than e-money products. In light of this, the level of the money laundering threat related to e-money is considered as significant (level 3).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to e-money made the following findings:

a) risk exposure

The e-money sector is not homogeneous, due the wide range of products in which the level of terrorist financing and money laundering risks are completely different. Some e-money products that are not linked to a current account (cash-based products[40]) offer anonymity features similar to cash because they are exempt from customer due diligence measures. The terrorist financing inherent risk can be significant in these specific e-money products due the low amounts used in terrorist attacks and because they offer a discrete way to make low payments in comparison with cash. Nevertheless, perpetrators still consider the use of cash as a preferred option due to the complete anonymity.

The terrorist financing inherent risk for non-cash-based e-money products can be considered similar to that for other banking products or credit cards. Despite the origins of funds being known and traceability of payments being complete, perpetrators can use these products as a means of payment even if they have to pass customer due diligence measures. This is because most of the time perpetrators are not under the scope of sanctions regime.

In respect of TF, e-money products offer a more secure way of moving money to conflict zones for terrorist financing, but the use of such products as a means of payment in these areas can be more difficult.

Inherent risk depends mainly on the structure of the product, but even e-money products non-cash-based can present a significant risk if the funds are legitimate, perpetrators are

[40] E-money products loaded by cash not by a bank account or a credit card.

not on the sanction lists and the amounts of money needed are low. It is remarkable that financial sanctions target individuals or groups that are already known to pose a threat, whereas risk often emanates from individuals who are not caught by the sanctions regime. In that sense, the terrorist financing inherent risk is independent of the thresholds or the customer due diligence measures applied.

b) risk awareness

Sector awareness can be considered high, especially after some terrorist attacks where e money products were used. However, there are still some concerns among supervisors as to whether e-money firms who sell products with an exemption from customer due diligence are able to perform efficient monitoring and reporting of suspicious transactions. On the other hand, the results of thematic inspections to the sector has shown a good level of checks and risk assessment in the firms inspected. Most supervisors classify the sector's overall risk as 'moderately significant' or 'significant'.

There is an increasing number of initiatives aimed at engaging with competent authorities and law enforcement agencies; these can contribute to raising the risk awareness in the sector and to improving efficiency.

c) legal framework and checks

E-money is covered by AML/CFT requirements at EU level. Under the 5th AMLD, e-money products will benefit from an exemption regime which means that customer due diligence need not be applied when specific conditions are fulfilled. In addition, thresholds are lower than in the 4th AMLD that mitigate the anonymity of certain products. On the other hand, AML Directives require e-money issuers to carry out sufficient monitoring of the transactions to apply customer due diligence exemptions.

Having effective checks in place in relation to terrorist financing can require a lot of AML/CFT staff, which can affect the business model of small e-money firms and reduce the efficiency of their monitoring systems, even when they have proper software tools to monitor transactions. In that sense, when it comes to terrorist financing risks, the efficiency of checks is independent of the customer due diligence measures applied and depends more on the quality of the databases checked to detect transactions and customers linked with terrorist financing. The sector's engagement with competent authorities and law enforcement agencies is crucial to improve efficiency and mitigate such risks.

Conclusions: The lower thresholds set out in the 5th AMLD will reduce the anonymity of the riskiest products and therefore the vulnerability of the sector. Risk awareness has improved, as has been confirmed by some supervisors, but there are still some concerns about the efficiency of their systems to monitor and report suspicious transactions linked with terrorist financing activities. In this context, the level of terrorist financing vulnerability related to e money is considered as significant (level 3).

Money laundering

The assessment of the money laundering vulnerability related to e-money shows made the following findings:

a) risk exposure

Among the wide range of e-money products, the products most exposed to money laundering risks are the ones that can be purchased for cash. The use of these products individually for money laundering purposes is costly because of the lower thresholds and the cost of hiring frontmen to circumvent the thresholds for applying customer due diligence. However, when some intermediaries act in the delivery channel of the e-money product (distributors, agents), this can be the weakest part of the AML prevention system if firms are unable to perform efficient monitoring of their distributor's network.

Perpetrators or facilitators can have an external agreement with these agents or distributors to purchase large amounts of prepaid cards and move those funds across Member States or non-EU countries, or even to sell such amounts of prepaid cards at a discount to third parties. If e-money firms do not have robust checks over their distributor's network and detect potential rogue distributors, such distributors will be able to avoid applying customer due diligence measures properly and to introduce fake documents into the system, in a similar way as occurs with rogue agents of money remittance firms. As a consequence, the risk inherent in distribution models is determined primarily by the extent to which e- money is distributed by persons other than the e- money issuer.

The money laundering inherent risk is considerably lower for the remaining e-money products linked to a bank account or a payment account.

b) risk awareness

The sector trusts in the use of technology for its checks over e-money products and asses the money laundering risk posed by its products, even pre-paid cards or cash-based vouchers, as 'less significant' or 'moderately significant'. The issuer of the e-money has access to the product at every moment and has resources to deactivate cards in case of suspicious transactions. Most supervisors have assessed the sector's overall risk profile as 'moderately significant' or 'significant'. The difference in perception between the sector and supervisors stems mainly from divergent views of the extent to which e-money issuers' AML/CFT checks are effective. On the other hand, in one EU Member State where many licences have been issued, the supervisory authority has recently conducted a thematic inspection in the sector and has found a good level of checks and risk assessment in the firms inspected.

c) legal framework and checks

E-money is covered by AML/CFT requirements at EU level. Under the 5th AMLD, e-money products benefit from an exemption regime which means that customer due diligence requirements need not be applied when specific conditions are fulfilled. In addition, thresholds are lower than in the 4th AMLD that mitigate the anonymity of

certain products. On the other hand, AML Directives require e-money issuers to carry out sufficient monitoring of the transactions to apply customer due diligence exemptions.

Supervisors identified weaknesses in particular in the effectiveness of monitoring, the identification of suspicious transactions, and internal checks and oversight. However, the sector relies heavily on transaction monitoring as a risk mitigation tool, which includes effective distributor's network oversight. However, it is worth noting that large distributor's network oversight may require additional staff in addition to technology, and that increase vulnerability in small e-money firms.

Conclusions: e-money cash-based products are more vulnerable than other bank account-based e-money products because of the higher level of anonymity. The level of money laundering awareness in the sector is high, but there are still some doubts among supervisors about monitoring systems, specifically in connection with large distributor's networks and with cash-based e-money products. In this context, the level of money laundering vulnerability related to e-money is considered as moderately significant/significant (level 2/3).

Mitigating measures

For Member States / competent authorities:

- transposition of the 5th AMLD provisions related to e-money;
- thematic on-site inspections focusing on the risk posed by distributors.

9. Transfers of funds

Product
Transfers of funds

Sector
Credit and financial institutions — money value transfer services

General description of the sector and related product/activity concerned
Money value transfer or money remittance is defined under the second Payment Services Directive (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 payment service providers including credit institutions, e-money institutions, and authorised payment institutions.. Money remittance is the payment service for which authorised payment institutions are most commonly authorised for.

According to general ECB statistics, in 2017 the total amount of remittances sent from EU Member States amounted to €270 billion, but this figure does not include the UK, Luxembourg, Poland, Slovakia, Denmark, Cyprus and Finland. This figure only shows a slight increase compared to 2016 (€240 billion).

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

Terrorist financing

Perpetrators use money and value transfer 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 value transactions to avoid raising red flags.

Money laundering

Perpetrators may use MVTS services to carry out a number of illicit operations. These are listed below.

- Transfer of funds from legitimate and illegitimate customers. Rogue agents usually perform transactions using fake IDs and fake invoices.
- Proceeds of crime are laundered through settlement systems in a non-EU country (using passporting). MVTS providers channel funds through highly complex payment chains with a high number of intermediaries and jurisdictions involved in the funds circuit, hindering the traceability of illicit funds. MVTS providers operating along 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.
- Large sums of cash are broken down into smaller amounts that are below the thresholds for which stricter customer identification is required.
- Proceeds of crime are placed in the financial system through a regulated MVTS offering payment accounts or similar products. Perpetrators may also use such regulated MVTS providers to channel their funds.
- Funds are placed and/or transferred through money remittance services. Risks of money laundering / terrorist financing activity may be particularly high when funds to be transferred are received in cash or in anonymous e-money.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to money value transfers services shows that terrorist groups recurrently use this method. Law enforcement agencies and financial intelligence units have gathered strong evidence that these services are used to collect and transfer funds used to support the financing of terrorist activities within the EU and in particular to transfer funds by/for foreign terrorist fighters travelling to/from conflict zones.

MVTS providers 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 large MVTS providers due to their global network of agents, while smaller MVTS providers might not be so attractive since they usually operate in a limited number of countries. The specific features of MVTS providers (see vulnerabilities part) mean that they are perceived as attractive and secure.

Conclusions: MVTS providers are frequently used to finance terrorist activities and do not require specific knowledge or planning. In light of this, the level of the terrorist financing threat related to MVTS is considered as very significant (level 4).

Money laundering

Organised crime groups recurrently use this method. Law enforcement agencies and financial intelligence units have gathered strong evidence that these services are used to collect and transfer funds used to support money laundering activities. MVTS providers are, depending on their organisation, easy to access and do not require specific expertise or techniques to launder proceeds of crime. The specific features of MVTS providers mean that they are perceived as attractive and secure. Usually perpetrators get in touch with agents to launder the money of an organised crime group in exchange for a percentage of the amount of money laundered. Agents linked with these perpetrators usually perform fake transactions with fake customer IDs if they are aware of weak customer due diligence checks by the MVTS firm. Otherwise, they can use real customer forms to add new transactions.

Based on the principle of non-exclusivity, agents can work for different companies at the same time. This means that when they are connected with perpetrators, agents can easily split transactions between firms in order to launder large amounts; such activities are difficult to detect for individual firms and competent authorities.

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

Vulnerability

Terrorist financing

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. When money is used for terrorist attacks in the EU, a higher inherent risk results from the sending of low amounts and from payers who are not included on sanctions lists.

The sector is vulnerable to cross- border abuse for terrorist financing purposes. Investigations carried out by law enforcement agencies following recent terrorist attacks, for example in Paris and the UK, have confirmed that terrorists used money remittance to raise and move funds. In contrast to money launderers, individuals looking to finance terrorism may not seek to hide their identity and may use legitimate funding sources, often in small amounts. Additionally, the terrorist financing risk often emanates from individuals who are not covered by the sanctions regime.

The significant risk of money laundering and terrorist financing in the MVTS sector has led banks to adopt ‘de-risking’ policies towards money remittance services in certain higher risk regions. This trend raises concerns, as de- risking may ultimately lead to money remittance services being driven underground (i.e. informal service providers such as hawala services). Financial inclusion concerns also arise, as money remittance services play an important role for customers who have limited or no access to other regulated financial services.

b) risk awareness

According to the competent authorities, risk awareness in the sector is high (due to the recent terrorist attacks), but the measures firms put in place to identify their customers and verify their identities may carry less weight in the counter-terrorist financing context than effective ongoing monitoring of transactions. Law enforcement agencies notice that the bigger players are more often misused by terrorists than the smaller ones due to their bigger agent networks in different countries.

The fight against terrorist financing continues to be hampered when firms do not have access to relevant information, often held by law enforcement agencies, that would help them identify terrorist financing risks before they materialise. Likewise, law enforcement agencies' efforts to disrupt terrorist activities and networks can be hampered when they are unable to obtain information about finance flows that only firms can provide.

The majority of supervisors consider the overall risk profile of the sector as significant or very significant, and more than 50% of the firms in the sector are rated as a very significant risk.

c) legal framework and checks

Registered and authorised MVTS providers are subject to AML/CFT requirements at EU level. The effectiveness of checks in place is rated by supervisors mainly as poor. Firms in the sector, especially large firms, rely on their customer checks and alert systems to mitigate risks.

The efficiency of current systems to detect suspicious transactions linked to terrorist financing is not high, despite their being intensive in human resources. As with inherent risk, terrorist financing risk often emanates from individuals who are not covered by the sanctions regime. As a result, closer cooperation is needed between firms and law enforcement agencies so that they become more efficient at detecting customers linked to terrorist activities.

Conclusions: MVTS vulnerability to terrorist financing is high. This is because the features of transactions linked to terrorist financing are not easily detectable, despite human and technical resources put in place by firms. The effectiveness of checks depends on the sources of information used to check transactions and customers. Firms and law enforcement agencies need to improve exchange of information to enhance detection of suspicious transactions linked to terrorist financing. In light of this, the level of terrorist financing vulnerability related to MVTS is considered significant/very significant (level 3/4).

Money laundering

Money laundering vulnerability related to money value transfers services cannot be assessed without considering that most MVTS providers rely on agents. Therefore agents constitute the main factor for risk exposure for MVTS providers.

a) risk exposure

MVTS services are, in a number of cases, cash-based and allow for speedy transactions. Due to their specific features and in particular their reliance on agents, MVTS services can be provided in high-risk non-EU countries and may be used by high-risk customers meant to be subject to specific monitoring and checks. Therefore, the most prevalent risks in the MVTS sector are the cash-intensive nature of the service, the high speed and volume of transfers, (although individual transactions are usually low), and transfers to high-risk jurisdictions.

Performing consistent customer due diligence can be problematic due to the nature of the customers, who usually make isolated transactions, and due to the risk that frontmen will be used to perform transactions (despite this being a more expensive method to launder money). However, inherent risk is higher when money remittance firms has not robust monitoring systems to check retail agents' networks, especially in firms with large retail agent's networks.

The significant risk of money laundering and terrorist financing in the MVTS sector has led banks mainly to adopt 'de-risking' policies towards money remittance services in certain higher risk regions. This trend raises concerns, as de- risking may ultimately lead to money remittance services being driven underground (i.e. to informal service providers such as hawala services). Financial inclusion concerns also arise, as money remittance services play an important role for customers who have limited or no access to other regulated financial services.

b) risk awareness

Risk awareness can be considered high in the sector. Checks are in general effective when focused on customer risk; however, when it comes to the money laundering risk from rogue agents, checks are not so effective across the EU. In addition, in some countries thresholds are in place for customer due diligence obligations that make it more difficult to conduct proper oversight of agents. In that sense, it is also noteworthy that the sector is very competitive and there are low profit margins, therefore sometimes there is a trade-off between profitability and compliance. Agents linked with money laundering activities are usually the most profitable ones. Hence, if firms are not able to detect a clear connection with such activities, they prefer to keep the agent in their networks but under surveillance (usually setting quantitative limits for their transactions), rather than report the agent to the financial intelligence unit and thus break the commercial relationship.

Supervisory awareness of such risks is high. In their risk assessments, some supervisors have cited the following risks associated with agent networks: inadequate agent governance, training and monitoring. In contrast, most supervisors perceive the sector's awareness as poor or very poor.

Reporting of suspicious transactions to financial intelligence units is not always effective if firms report large amounts of isolated customer transactions instead of reporting agents or groups of agents performing those transactions.

c) legal framework and checks

Registered and authorised MVTS providers are subject to AML/CFT requirements at EU level. Because of the reliance on agents, supervision of the sector is very challenging. Firms rely on new technologies and software to conduct robust customer due diligence and agent oversight, but because of the specific features of their customers, such measures are not always efficient. MVTS providers need training to perform proper customer due diligence but such training is not efficient when it comes to addressing the risk posed by rogue agents.

Currently, cross-border cooperation is not working properly and supervisors are not able to put in place appropriate checks and an appropriate sanctions regime. That being the case, one of the aims of the 4th and 5th AMLDs is to enhance cooperation between AML supervisors. In this light, setting up 'AML colleges of supervisors' when obliged entities operate in different jurisdictions can improve supervision across EU.

Conclusions: Inherent risk is high, but risk awareness in firms is growing. Supervisors and firms are addressing the money laundering risk, focusing their actions on areas of higher vulnerability such as oversight of agents. However, to reduce vulnerability some improvements are still needed, such as enhanced supervisory cooperation, and more effective customer due diligence and oversight of agents. In this context, the level of money laundering vulnerability related to MVTS is considered as significant (level 3).

Mitigating measures

For Member States / competent authorities:

- Member States should eliminate thresholds to occasional transactions, applying customer due diligence to all transactions, so that MVTS firms can efficiently monitor and detect suspicious transactions and suspicious agents linked to money launderers.
- Set up and promote a system in which suspicious agents reported by MVTS firms are recorded in a database to which all firms in the sector have access. This would limit or eliminate the activity of suspicious agents.
- Competent authorities should conduct a number of on-site thematic inspections focusing on risks posed in agents. The scope of these thematic inspections should include checking that MVTS firms have a comprehensive agent oversight function including efficient monitoring systems, on-site reviews and training.

For the European supervisory authorities:

- Encourage competent authorities to dedicate appropriate resources, proportionate to the level of risks, to MVTS inspections, focusing on oversight of agents.

For the Commission:

Promote cooperation between law enforcement agencies and financial institutions in order to improve effectiveness of terrorist financing alert systems at supranational level.

10. Illegal transfers of funds — Hawala

Product
Illegal/informal transfer of funds through hawala

General description

Hawala is a system of money transmission which arranges the transfer and receipt of funds or equivalent value. It is often reliant on ties within specific geographical regions or ethnic communities. These movements of value may be settled through trade or cash businesses engaged in remittance activities. They often operate in areas of expatriate communities. *Hawaladars* (those that operate hawala) often run parallel businesses, particularly currency exchange, travel agencies or telephone shops, or even work as agents of official money transfer providers. The term hawala is often used to describe a number of different informal value transfer systems which have similar properties and operate in similar ways, although they are not strictly hawala. Such fund transfers are considered as unregulated payment services under EU law, meaning that they are illegal within the EU. Informal systems of value transfer, like *Hawala*, can be used for legitimate purposes, like money remittances, but also for criminal ones.

In 2013, the Financial Action Task Force (FATF) came up with the wider term 'Hawala and other similar service providers' or 'HOSSPs' to describe this activity. HOSSPs are a subset of informal value transfer services; forms other than hawala include hundi, Chinese underground banking and black market peso exchange. Informal value transfer systems are concerned with the movement of value without the need for money to be physically or electronically moved.

Members of diaspora and migrant communities use HOSSPs extensively to send legitimate remittances to their country of origin. At the same time, the implementation of stricter anti-money laundering regulations in mainstream financial institutions has also made informal value transfer systems, and HOSSPs increasingly attractive to organised crime groups, who frequently use them to transfer illegitimate remittances, i.e. transfer large amounts of criminal proceeds or to launder such criminal proceeds, providing layering and remittance services within and outside 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. Instead, as is also often the case in money remittances, this is done by offsetting balances between the hawaladar of the payer and the hawaladar of the payee. To illustrate this method, 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.

Normally, all operators providing payment services as defined in Annex I, point 6 of the second Payment Services Directive (PSD2) should be appropriately registered and

regulated. Such providers should seek the status of authorised payment institutions. Recent and significant law enforcement efforts have proved beyond doubt that the unregulated and clandestine nature of HOSSP informal remittance systems has made them the preferred choice of criminals in money laundering.

Although hawaladars must be registered and properly licensed under the Payment Services Directive, these payment service providers often choose to carry out such transfers irregularly, outside of the conventional banking system and without proper licensing. This means that they circumvent their anti-money laundering obligations and avoid mandatory supervision under the anti-money laundering regulations. Often authorities lack the means to detect these networks and properly enforce the application of PSD2 and AML obligations to these providers.

Description of the risk scenario

Contrary to all other remittance systems, hawala is based on a network of key players (hawaladars) tied by trust due to specific geographical regions, families, tribes, ethnic communities, nationalities, commercial activity, etc. Hawaladars settle transactions between themselves over a long period of time by net settlement using banking channels, trade or cash. This means that contrary to all other remittance systems, funds are not transferred for each and every transaction. Instead, each day they use a local cash pool with money that was already in the system to pay the beneficiary. After a set period (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. It needs to be stressed that legitimate and licensed value transfer services also usually operate in this way.

The hawala network also uses some unique techniques:

- bilateral settlement: ‘reverse hawala’ between two hawaladars;
- multilateral settlement: ‘triangular’, ‘quadrangular’ or other arrangements between several hawaladars in the same network;
- value settlement through trade transactions, usually applying trade-based money laundering techniques (shipment of the equivalent value through trade transactions such as merchandise, paying a debt, or invoice of same value that they owe. Over-invoicing or under-invoicing. Double invoicing. Black market peso exchange, etc.);
- cash settlement via cross-border cash couriers, banking and money service business channels.

Specific hawala networks are created to serve exclusively criminal needs; these place and layer criminal money and pay the equivalent value on demand elsewhere in the world. Such networks are known to use the techniques described above. In addition, to protect themselves, hawala networks use the following techniques:

- quick cash pick-ups;

- authentication via a token (a regular feature of criminal cash handovers is the use of the unique serial number on a banknote to act as a means of identification and a rudimentary receipt for the handover);
    - placement via cuckoo smurfing (a form of money laundering linked to alternative remittance systems in which criminal funds are transferred through the accounts of unwitting persons who are expecting genuine funds or payments from overseas).

    All these techniques are unique to the hawala system and are all known red flag indicators of hawala activities for EU law enforcement agencies.

    Such criminal hawala networks also follow a particular structure composed of:

    - controllers or money brokers — these make the deal with organised crime groups for the collection of dirty cash and for delivery of its value to a chosen destination;
    - coordinators — these are intermediaries working for the controller and managing different collectors;
    - collectors — these collect dirty cash from criminals and dispose of it;
    - transmitters — these receive and dispatch the money obtained by the collector (usually a money service business operator).

Threat

The scale of *hawala* in the EU is unknown.

Hawala is known to be associated with certain businesses of certain ethnic communities (India, Afghanistan, Pakistan, Iran, United Arab Emirates, Somalia and China) that are common in the EU. Examples of the kinds of business involved are travel agencies, pawn shops, mobile phone and SIM cards sales, top-up of mobile cards, grocery stores, import/export business, as well as various neighbourhood-type businesses such as nail salons, hairdressers, beauty salons, flower shops.

Europol is also aware of several ongoing multi-million euro money laundering investigations focusing on criminal *hawala*.

There are no direct money/value flows between sender and receiver that law enforcement agencies can track or trace. This makes tracing the money/value flow in a hawala network virtually impossible even if ledgers are seized — they are usually encrypted, and more and more often located on cloud servers located in non-cooperative jurisdictions. This opacity makes it attractive for perpetrators.

LEAs have detected some overlap between official and informal value transfer systems, notably through “cuckoo smurfing”. On the other hand, *hawaladars* are able to launder large sums of cash for different proceeds of crime (drug trafficking, tax evasion, terrorist financing, etc.). A collector/hawaladar receives commission ranging from 2% to 10%.

Vulnerability

Such illegal fund transfers are considered as unregulated payment services under EU law, meaning that they are illegal within the EU. There is no specific vulnerability assessment for illegal services in the context of the supranational risk assessment report.

Mitigating measures

For Member States / competent authorities:

- Set up joint money laundering intelligence task forces. Ensure cooperation between the financial sector and government institutions on the exchange of intelligence to prevent money laundering (which may also extend to hawala services).
- Carry out supervisory actions to verify that obliged entities, especially money remitters, have in place checks to detect hawaladars using registered agents as window dressing to attract customers in order to offer them hawala.

11. Payment services

Product
Payment services

Sector
Credit and financial sector

General description of the sector and related product/activity concerned

Payment services products

Payment services are regulated by the revised Payment Services Directive (2015/2366) ('PSD2'). They are listed in Annex I of PD2 and cover a wide variety of services, including:

- services enabling cash to be placed on or withdrawn from a payment account (cash deposits are addressed in a separate section of this report);

- money remittance (also covered in another section of this report);

- execution of payment transactions such as credit transfers or direct debits;

- execution of payment transactions through payment cards or similar devices;

- issuing of payment instruments;

- acquiring of payment transactions.

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.

PSD2 covers additional payment services, which have emerged during the past years in the slipstream of the digitalisation of services. These services are referred to as payment initiation services and account information services. When assessing the relevant money laundering risk, only payment initiation services are relevant.

Payment initiation services allow consumers to pay for their 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 payment initiation service provider can check if there are sufficient funds on the consumer's account balance to make the payment. It informs the merchant that the payment order has been successfully initiated. On that basis, the web merchant may decide to ship the goods or render the service before the amount is booked on his account. PSD2 covers these new payments, addressing potential issues over confidentiality, liability and the security of such transactions.

PSD2 became applicable on 13 January 2018. As of 8 February 2019, 25 Member States communicated full transposition of the Directive, two (Malta and Spain) partial transposition and in Romania the Directive is not yet transposed.

PSD2 does not regulate all payments. Payments in cash or paper cheque payments are not covered. Payments transactions by a provider of electronic communication networks, under a certain value are also excluded from the scope of the Directive.

The large majority of payments is done electronically. The total number of non-cash payments in the EU increased by 7.9% to €134 billion in 2017 compared with the previous year, as follows:

- payments with credit and debit cards accounted for 52% of all transactions;
- credit transfers accounted for 24% and direct debits for 19%;
- the number of credit transfers increased by 5.5% to €32.1 billion.

The number of cards with a payment function in the EU increased in 2017 by 2.0% to 812 million. With a total EU population of 513 million, this represented around 1.6 payment cards per EU inhabitant. The number of card transactions rose by 11.2% to 69.2 billion, with a total value of €3.1 trillion. This corresponds to an average value of around €44 per card transaction.

SEPA

The Single European Payments Area (SEPA) aims to harmonise and integrate payment markets across Europe, with one set of euro payment instruments: credit transfers, direct debits and payment cards, common standards and practices, and a harmonised legal basis. SEPA covers more than 520 million people in the 28 EU Member States and six non-EU countries (Iceland, Liechtenstein, Monaco, Norway, San Marino and Switzerland).

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 2017, 43 retail payment systems existed in the EU as a whole. During that year, around 57 billion transactions were processed by those systems, covering €44.0 trillion. Some 22 of these systems were located in the euro area, where they processed almost 42 billion transactions in 2017 (i.e. 73% of the EU total), covering a value amounting to €31.6 trillion (i.e. 72% of the EU total).

Large-value payment systems

Large-value payment systems are designed primarily to process urgent or large-value interbank payments, but some of them also settle a large number of retail payments. During 2017, 12 systems settled 842 million payments with a total value of €702 trillion in the EU. The two main large-value payment systems in the euro area (TARGET2 and EURO1/STEP1) settled 143 million transactions amounting to €528 trillion in 2017, i.e. 75% of the total value.

Payment service providers

Banks are players in national and international payment systems. Some 122 billion cashless payments were made by non-monetary financial institutions in 2016 at EU-28 level. More than half (60 billion) of those were card payments, while about a quarter were credit transfers (31 billion) or direct debits (25 billion).

Within the EU, not only credit institutions are allowed to provide payment services. These can also be provided by e-money institutions, post giro institutions and regional or local authorities where they do not act as public authorities. In addition, with the adoption of the first Payment Services Directive in 2007, a new entity, 'payment institutions', was introduced. These can only provide payment services; they are not allowed to take deposits or issue e money. Under the second PSD, new categories of payment service providers were introduced: payment initiation service providers and account information service providers. They can provide exclusively the services of payment initiation and account information respectively.

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

The majority of payment service providers still consists of credit institutions.

As for the smaller players, EU-wide (status 2012) there were:

- 568 authorised payment institutions;
- 2,203 small payment institutions (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 (authorised payment institutions and small payment institutions) 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 authorised payment institutions 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 authorised payment institutions in the EEA. As for the small payment institutions, 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.

More general data on the number of financial institutions providing payment services in the EU can be found in the ECB Payments statistics report 2017: http://sdw.ecb.europa.eu/servlet/desis?node=1000001384.

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 terrorist financing 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 legislation) that may lead terrorists to use a false identity. This means that law enforcement agencies cannot track the originator or beneficiary of the transaction. The use of payment services requires specific skills but, according to law enforcement agencies, these skills are commonly widespread within terrorist groups and do not constitute an obstacle (mobile/internet payments are quite easy). The amounts concerned appear 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. Nevertheless, the amounts concerned remain quite limited. In this context, the level of terrorist financing threat related to payment services is considered as significant (level 3).

Money laundering

The assessment of the money laundering threat related to payment services is considered as presenting similarities with deposits on account. This risk scenario concerns both the placing and withdrawing of funds (i.e. deposits on account and use of this account). It is frequently used by criminals, but also by relatives/close associates, which extends the scope of the intent and capability analysis.[41] The funds used in payment services are from non-legitimate origins. It requires some planning and knowledge of how banking systems work.

[41] On intent and capability see footnote 34.

According to law enforcement agencies, payment services providers (PSPs) can be used by money mules, or can be criminally controlled:

> For example, a PSP has been investigated by several EU Member States. The PSP registered in one EU Member State registered as an e-money issuer in another jurisdiction and thus obtained a passporting licence. The PSP was approached by a criminal structure claiming to conduct online trade. The PSP supplied the client with point of sale terminals. The terminals were taken out of Europe and used in black peso market exchange 'swipe out' operations. The information collected in the investigations demonstrated that the PSP did not perform any monitoring of the client, which would have resulted in identification of the risk because the declared small online business led to the accumulation of several million euro in a limited amount of time. Nor were the point of sale terminals monitored, as they were physically not present in the EU for when the order was placed. The same PSP was also approached by another criminal structure in another EU Member State. The criminal structure controlled front tourist businesses used to make cash deposits of cocaine proceeds. These businesses became clients of the PSP and requested to be issued with bank cards (as the PSP is a Visa and Mastercard card issuer). The cards were taken out of Europe and cash was withdrawn in Colombia.

Conclusions: organised crime groups use this method rather frequently as it is easily accessible, despite requiring some knowledge and planning capabilities to hide the origin of funds. However, when criminal structures take over payment services providers, the money laundering risk can be higher. In this context, the level of the money laundering threat related to payment services is considered as significant (level 3).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to payment services has some features in common with the assessment of terrorist financing vulnerability concerning retail payment services.

a) risk exposure

The risk exposure is inherently high due to the characteristics of payment services, as they involve very significant volumes of products and services. Although payments are generally not anonymous (as they are linked to an identified account), they may interact 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 they imply a non-face-to-face business relationship.

b) risk awareness

The risk awareness is generally good because the sector has put in place guidance to detect the relevant red flags on terrorist financing. This is confirmed by a good level of reporting, as the sector seems to have adequate tools to detect these risks. However, customer due diligence 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 of the vulnerabilities of the sector and are proactively engaged with it.

c) legal framework and checks

Payment services are included in the AML/CFT legal framework at EU level. This framework has been in place for many years and checks are considered overall to be efficient. As far as the legal framework is concerned, it covers equally credit and payment institutions. Similar to deposits on accounts, checks in place are generally considered as efficient, however, sanctions screening is not a substitute for effective counter-terrorist financing checks. Financial sanctions target individuals or groups that are already known to pose a threat, whereas terrorist financing risk often emanates from individuals who are not caught by the sanctions regime. This is why risk- based AML/CFT checks, and transaction monitoring in particular, are key to an effective fight against terrorist financing.

Usually, banks and payment institutions do not have access to relevant intelligence, often held by law enforcement agencies, that would help them identify terrorist financing risks before they materialise. Likewise, law enforcement agencies' efforts to disrupt terrorist activities and networks can be hampered when they are unable to obtain information about finance flows that only firms can provide. There are now initiatives at the national and supranational level designed to test how law enforcement agencies can provide firms with more specific and meaningful information on specific persons of interest, allowing firms to focus their transaction monitoring on these persons.

Conclusions: The risk exposure may be considered quite high (significant level of transactions). The sector shows a good level of awareness of the risk vulnerability and is able to put in place the relevant red flags. The legal framework and checks are the basis of a good level of reporting. However, residual risk is high due to the reliance on the current counter-terrorist financing checks based on sanctions screening. In this context, the level of terrorist financing vulnerability related to payment services is considered as significant (level 3).

Money laundering

The assessment of the money laundering vulnerability related to payment services has some common features with the assessment of money laundering vulnerability related to retail services.

a) risk exposure

Risk exposure is inherently high due to the characteristics of payment services which often involve very significant volumes of funds. Although payments are generally not anonymous (as they are linked to an identified account), they may entail contact with higher risk customers or countries, especially where cross-border movements of funds

are involved. They also make use of new payment methods (mobile/internet), which may increase the level of risk exposure because they imply, a non-face-to-face business relationship.

b) risk awareness

Competent authorities have noted discrepancies between banking and payment institutions, the latter being less aware of money laundering risks. Most competent authorities viewed the overall risk profile of payment institutions as either significant or very significant; this was especially the view of the authorities supervising the highest numbers of payment institutions. The potential misuse of new technologies such as mobile payments to facilitate peer- to- peer money transfers was commonly considered as an emerging risk by competent authorities (see the section on virtual currencies). There is currently insufficient monitoring both when a payment account is opened (entry point) and when the transaction is processed.

c) legal framework and checks

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 the banking sector and to the payments institutions sector. This framework has been in place for many years and checks are considered overall as efficient. Payment institutions rely on bank controls to mitigate their inherent money laundering risk, but some alert systems in banks are not robust enough to detect suspicious cash transactions transferred by payment institutions afterwards.

Conclusions: The sector's risk exposure and risk awareness are quite similar to those for the deposits on accounts. As far as the legal framework is concerned, it covers equally bank and payment institutions. However, the checks in place are less efficient when dealing with payment institutions. In this context, the level of money laundering vulnerability related to payment services is considered as significant (level 3).

Mitigating measures

For the Commission:

- clarify and set up a common framework for electronic identification and customer due diligence;
- identify risks associated with Fin-Tech and set up standards to mitigate those risks;
- carry out a study mapping and analysing on-boarding bank practices across the EU and assess any next steps
- promote cooperation between law enforcement agencies and financial institutions in order to improve effectiveness of terrorist financing alert systems at supranational level.

For Member States / competent authorities:

- Member States should ensure that supervisors conduct a number of on-site thematic inspections focusing on risk assessments of payment institutions, and ensure that their alert systems are effective.
- In addition, competent authorities should provide further risk awareness and risk indicators relating to terrorist financing.
- Member States should eliminate thresholds for occasional transactions, applying customer due diligence to all transactions so that payment institutions efficiently monitor and detect suspicious transactions.

12. Virtual currencies and other virtual assets

Product
Virtual currencies and other virtual assets

Sector
Virtual currencies and other virtual assets – service providers

General description of the sector and related product/activity concerned

Definitions

For the first time, the 5th Anti-Money Laundering Directive (AMLD5) introduced in EU law a definition of virtual currency (VC), which it describes as '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'.[42] AMLD5 specifies as obliged entities for AML/CFT purposes providers engaged in exchange services between virtual currencies and fiat currencies and virtual currency custodian wallet providers. In October 2018, FATF amended its standards extending Recommendation 15 (new technologies) to 'virtual assets' and 'virtual asset service providers'. The ammended recommandation 15 requires the countries and jurisdictions to regulate virtual asset service providers for AML/CFT purposes, to license or register them and to subject them to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

Additionally, Virtual assets (VAs) are now defined in the FATF glossary as 'a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes, and that does not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'.

The new FATF definition is broader than the AMLD5 definition of 'virtual currency'.

Furthermore, as a result of the changes, jurisdictions are recommended to have within the scope of AML/CFT obligations any natural or legal person (not covered elsewhere under the FATF Recommendations) who, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- exchange between virtual assets and fiat currencies;
- exchange between one or more other forms of virtual assets;
- transfer of virtual assets;

[42] Recital (10) of the AMLD5 makes clear that virtual currencies should not be confused with (among others): electronic money within the scope of EMD2 nor with funds within the scope of the PSD2: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN .

- safekeeping or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Stakeholders

Various stakeholders are involved in the VCs/VAs market, the main ones being:

- **wallet providers:** cryptocurrency users may hold VC/VA accounts on their own devices or entrust a wallet provider to hold and administer them (in an e-wallet) and provide an overview of the user's transactions (via a web- or phone-based service). There are three types of wallet provider:

    - hardware wallet providers, which provide users with specific hardware solutions to store their cryptographic keys privately;
    - software wallet providers, which provide users with software applications that allow them to access the network, send and receive cryptocurrencies, and save their cryptographic keys locally; and
    - custodian wallet providers, which take online custody of a user's cryptographic keys (including multi-signature wallets).

    Unlike software wallet providers (which provide applications or programs that run on users' hardware – computer, smartphone, tablet, etc. – and access public information from a distributed ledger and access the network), custodial wallet providers take custody of the user's public and private key. This is analogous to a traditional bank providing a personal account.

    Wallets can be stored online ('hot storage') or offline ('cold storage'), with the latter ensuring greater protection.

    Only custodian wallet providers ('entities that provide services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies') are obliged entities under AMLD5.

    Hardware and software wallet providers do not safeguard keys on behalf of their customers, but provide them with the tools to safeguard their cryptocurrencies themselves; this creates scope for possible ML/TF activities;

- **exchange platforms** (a person or entity engaged in the exchange of VC/VA for fiat currency, fiat currency for VC/VA, funds or other brands of VC/VA): these platforms (the *bureaux de change* of the VC/VA world) may accept a wide range of payments, including cash, credit transfers, credit cards and other VCs/VAs. They include cashpoint machines.

    Like traditional currency exchanges, large VC exchanges provide an overall picture of changes in a VC's exchange price and its volatility. Some platforms offer services such as conversion services for merchants who accept VC payments, but are afraid of depreciation and want to convert them immediately

into a (national) fiat money. AMLD5 covers only exchanges of VCs into fiat currencies, not into other VCs/VAs;

- **user** (a person or legal entity who obtains a VC amount 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 holds the VC for other purposes, such as investment): typically, users obtain VC in one of the following ways:
    - through an exchange (or, for most centralised VCs, directly from the entity governing the scheme) using fiat currencies or another VC;
    - through specific activities, such as responding to a promotion, completing an online survey and 'mining' (running special software to solve complex algorithms to validate transactions in the VC system); and/or
    - from the scheme-governing entity, the issuer or other users acting for purposes other than their trade, business or profession;
- **miners:** in decentralised VC schemes, miners solve complex algorithms to obtain small VC amounts. 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, it is in a position to interfere with transactions, e.g. by rejecting transactions validated by other miners. Miners group into pools (Antpool, F2Pool, BitFury, BTCC Pool, BW.COM, etc.). Currently, most are located in China; and
- **initial coin offerors:** FATF's recently adopted definition of virtual asset service provider covers 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset'. Coin offerors are individuals or organisations who offer coins to cryptocurrency users on the coin's initial release, either against payment (e.g. through a crowdsale) or free of charge (e.g. as part of a specific sign-up programme, such as Stellar), normally to fund the coin's further development or boost its initial popularity. A coin offeror can be the same person as the coin inventor, or another individual or organisation.

AMLD5 has extended anti-money laundering obligations to 'providers engaged in exchange services between virtual currencies and fiat currencies' (exchange platforms) and custodian wallet providers, but does not cover all VA-related activities referred to in the new FATF definition of VA service providers, in particular exchanges from VA to VA and initial coin offerings (see **Legal framework and checks** below).

The VC/VA market in the EU

It is hard to compile official data on the VC market. The estimates below are based on information from various websites that track exchange volumes and prices, or conduct research. Estimates from market players tend to be lower than the statistics found online. Hence, the following statistics should reflect high, but balanced estimates:

Total VC wallets worldwide	13 million (Q4 2015)[43] – 7.4 million in Q4 2014
VC wallets in the EU	About 3 million
VC users worldwide[44]	1-4 million
VC users in the EU	About 500,000
VC miners worldwide	100,000[45]
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
Cashpoint machines worldwide[46]	571
Cashpoint machines in the EU	> 100
Daily VC transactions	> 125,000 (Bitcoin only – for 2015)
Merchants accepting bitcoins	110,000 (Q4 2015) – 80,000 in Q4 2014
Market capitalisation of VCs	€7 billion

Description of the risk scenario

Money laundering: VAs carry a significant ML/TF risk, due to the ease of transferring VA to different countries as well as the absence of homogeneous controls and prevention measures at the global level. Perpetrators use VC/VA systems to transfer value or purchase goods anonymously (cash funding or third-party funding through virtual exchanges).

Terrorist financing: VCs/VAs generally involve non-face-to-face customer relationships and may allow for anonymous funding or purchases (cash funding or third-party funding through virtual exchanges in which the funding source is not properly identified). They may also allow for anonymous transfers, if the sender and the recipient are not properly identified.

Threat

VC/VA-related activity represents a growing money laundering/terrorist financing threat. Financial intelligence units (FIUs) across the FATF global network have seen a rise in the number of suspicious transaction reports that relate to VC/VAs; this is likely to accelerate for EU FIUs after the deadline for transposing AMLD5.[47]

[43] http://www.coindesk.com/state-of-bitcoin-blockchain-2016/; see slide 8.
[44] At least one transaction per month.
[45] http://bravenewcoin.com/news/the-decline-in-bitcoins-full-nodes/
[46] http://coinatmradar.com/ (consulted on 4 February 2016).
[47] The Luxembourg FIU noted a 70% increase in suspicious transaction reports filed in relation to the use of VAs between 2017 and 2018.

Europol regards Bitcoin as the VC/VA of choice for the majority of criminals, but anticipates a more pronounced shift towards anonymity-enhanced VAs, which offer greater privacy, faster transaction times, lower transaction fees and less price volatility.

The use of other coins with greater privacy will slowly remove the need for dedicated mixing services. The two largest mixing services have already ceased operating (in 2017). Exchangers can now offer VC/VA to VC/VA transactions that obfuscate the transaction trail and decentralised mixers have also been used.

A particular set of challenges arises from VC/VA services provided by criminals or non-compliant entities:

- operators use criminal money to set up a VC/VA company that deposits criminal money or illegally obtained VCs/VAs in a cashpoint machine;
- individuals buy/sell large volumes of VCs/VAs for any asset 'over the counter' (no intermediation) without being registered as VC/VA service providers or advertising their services; and
- Payment services providers offering crypto cards were initially offered only for Bitcoin, but there has been a shift towards support of multiple VCs/VAs. They often register in jurisdictions with 'favourable' regulatory arrangements.

Law enforcement agencies also face particular challenges in collecting information when VC/VA exchanges take place in a country other than that in which the payer/payee is located (which itself may be anywhere in the world).

Many countries are concerned about the abuse of initial coin offerings (ICOs) and more broadly about a lack of awareness among issuers of securities tokens as to their AML/CFT obligations, particularly in jurisdictions that do not require businesses to maintain a physical presence for registration and licensing purposes.

Terrorist financing

The assessment shows that terrorist groups may have an interest in using VCs/VAs to finance terrorist activities. A limited, but growing number of cases related to VCs have been reported.[48] The Egmont Group of FIUs has detected cases of terrorist groups using VCs and groups are known to have given instructions on the internet (including via Twitter) on how to use VCs/VAs.

Conclusions: Law enforcement agencies have information according to which terrorist groups may be using virtual currencies to finance terrorist activities. Consequently, the terrorist financing threat related to virtual currencies is considered significant (level 3).

Money laundering

The assessment of the money laundering threat related to VCs/VAs shows that organised crime organisations may use them to access 'clean cash' (paying in and paying out). Not only cybercriminals use VCS/VAs – other organised crime groups such as drug

[48] Some cases of donation through crowdfunding requested in Bitcoin, citing 'support for widows, martyrs, Muslim groups', attempting to avoid clear terrorism finance linkage and advising the use of Bitcoin cashpoint machines.

traffickers use them to move and launder the proceeds of crime. VCs/VAs allow such groups to access cash anonymously and hide the transaction trail. Criminals may acquire private keys for e-wallets or withdraw cash from cashpoint machines.

Conclusions: An increasing number of investigations have concerned criminal organisations' (not only cybercriminals') use of virtual currencies and virtual assets. Consequently, the level of money laundering threat related to virtual currencies is considered significant (level 3).

Vulnerability

Terrorist financing

In assessing the terrorist financing vulnerability related to VC/VA providers, we must bear in mind that, while the EU has started to regulate VAs/VCs, the risks of their being misused to finance terrorism are only just emerging.

a) risk exposure

When used anonymously, VCs make it possible to conduct transactions speedily without having to disclose the identity of the 'owner'. They are provided through the internet and the cross-border element is the most obvious risk factor, as it allows for interaction with high-risk areas or high-risk customers that cannot be identified. This may change once the new FATF standards are implemented, as they will oblige VA service providers to register in the place of legal creation or incorporation (legal persons) or in the jurisdiction in which the place of business is located (natural persons). Nevertheless, the use of VCs/VAs is spreading fast and the number of transactions is expected to increase significantly in the coming years.

b) risk awareness

This component of terrorist financing vulnerability is difficult to assess in a comprehensive manner – while 'providers engaged in exchange services between virtual currencies and fiat currencies' and custodian wallet providers are now obliged entities at EU level, this is not (yet) the case for all VC/VA providers. Furthermore, competent authorities and financial intelligence units have noted in their contacts with the sector that the level of awareness of terrorist financing risk is still rather low, although the sector is calling for the adoption of an appropriate AML/CFT legal framework.

VAs are among the most important emerging risks in almost all sectors, due to:

- a lack of knowledge and understanding, which prevents firms and competent authorities from carrying out a proper impact assessment;
- gaps or ambiguities in the application of existing regulation';
- potential exposure of financial and credit institutions to increased risks of money laundering and terrorist financing related to VCs/VAs where they act as intermediaries or exchange platforms between VCs/VAs and fiat currencies (in the absence of a proper risk assessment); and
- in the investment sector, online processing of transactions with only limited customer identification and verification checks.

The sector is not well organised yet and it is difficult to find adequate tools to provide it with relevant information in order to increase the level of awareness.

c) legal framework and checks

AMLD5 has introduced a first EU definition of VCs and extended anti-money laundering obligations to 'providers engaged in exchange services between virtual currencies and fiat currencies' and custodian wallet providers. In addition to ordinary customer due diligence, Member States must ensure that these new obliged entities are registered. They must also require competent authorities to ensure that only fit and proper persons hold management functions in these entities or are their beneficial owners.

The latest changes to the FATF standards on VAs mean that the AMLD5 definition of VC may be too narrow, as it does not cover other kinds of VA.

In addition, there might be gaps to be filled as regards various activities of VA service providers that are not covered by the EU framework:

- custodian wallet providers that do not safeguard keys on behalf of their customers, but merely provide them with tools to safeguard their cryptocurrencies themselves, like hardware wallet providers and software wallet providers;
- exchanges from VCs or VAs to other VCs or VAs; and
- 'participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset', in particular in cases where the coin offeror may be the same person as the coin inventor, or another individual or organisation.

Conclusions: The most significant factor of vulnerability for virtual currency and virtual asset providers is the fact that they may not be fully regulated in the EU. Once implemented, AMLD5 will improve the situation considerably by making wallet providers and providers of exchange services between virtual currencies and fiat currencies obliged entities, ensuring that they are registered and that only fit and proper persons hold management functions or are beneficial owners. This framework still has to be implemented and it will be necessary to consider extending it to cover other virtual asset service providers, such as initial coin offerors and the providers of exchange services between virtual currencies. The inherent risk exposure is very high due to the characteristics of virtual currencies (internet-based, cross-border and anonymous). Finally, the sector is currently not organised well enough to receive guidance or relevant information on AML/CFT requirements. Consequently, the level of terrorist financing vulnerability related to virtual currencies is considered significant/very significant (level 3/4).

Money laundering

The assessment of money laundering vulnerability related to VC providers starts with the same caveat as for terrorist financing. They are partially regulated in the EU and there is little evidence of VCs being misused for money laundering. However, this does not prevent an assessment of potential vulnerabilities. Although few investigations lead to prosecution, the risk exists and can be analysed.

a) risk exposure

As mentioned above, when used anonymously, VCs make it possible to conduct transactions speedily and without having to disclose the identity of the 'owner'. They are provided through the internet and the cross-border element is the most obvious risk factor, as it enables interaction 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 new AMLD5 rules will address this by extending the AML/CFT framework to 'providers engaged in exchange services between virtual currencies and fiat currencies'. However, the delivery channels remain decentralised, which increases the risk exposure (in particular, cashpoint machines make it possible to withdraw or convert VCs).

b) risk awareness

This is emerging technology and the level of risk awareness in the sector is struggling to keep up. The sector is in more and more need of a legal framework in which VCs are subject to AML/CFT requirements. FIUs cannot detect and analyse risk on the basis of the blockchain alone. They cannot establish what sums are stored in e-wallets, nor identify the origin/beneficiary of the funds.

c) legal framework and checks

AMLD5 will add VC exchange platforms and custodian wallet providers to the list of obliged entities and make them subject to customer due diligence and compulsory registration. As with terrorist financing, improvements may be needed to ensure that all VC/VA providers meet AML/CFT requirements.

At the beginning of 2019, in the light of the latest changes to the FATF recommendations on VAs, the European Securities and Markets Authority and the European Banking Authority published reports on the adequacy of the current EU regulatory framework with regard to initial coin offerings and crypto-assets. They call for the scope of the AMLD to be reviewed in light of the new definitions of VA and VASP (FATF 2018). The new international standards require that the provision of these other VA service be regulated further and that the current definition of VC be adapted to encompass the broader realities covered by the term 'virtual assets'. Anonymity in some VA transactions also remains a major risk factor that could be addressed.

Conclusions: AMLD5 should significantly enhance the monitoring of risks linked to virtual asset service providers, but it has still to be implemented. The framework could also be extended to virtual asset service providers not yet covered (e.g. initial coin offerors and providers of exchange services between virtual currencies) and aligned with the new FATF standards. The inherent risk exposure should continue to be regarded as very high, due to the characteristics of virtual currencies (internet-based, cross-border and anonymous). Therefore, the level of terrorist financing vulnerability related to virtual currencies is considered significant/very significant (level 3/4).

Mitigating measures

- The Commission will assess suitable ways to complete its regulatory framework so as to ensure that VC/VAs and all VC/VA service providers are properly covered by anti-money laundering obligations.
- Competent authorities should monitor developments in this area closely and assess whether changes to national legal and regulatory AML/CFT frameworks are required.
- In 2022, the Commission will issue a report on the implementation of AMLD5 and efforts by MSs to implement the FATF standards.
- The Commission is currently assessing the financial services regulatory framework to make sure that is is effectively applicable to VAs that are covered by it as well as exploring whether legislative action is warranted for the VAs that do not currently fall within the financial services regulatory framework as these present very much the same risks as pointed out in the advice published by EBA and ESMA in January 2019.
- The Commission will continue to advocate a coherent, coordinated international regulatory framework around VC/VAs, building on its efforts in the G20 and international standard setting bodies. The Commission continues to be actively involved in the FATF work and has also joined the latest FATF private sector contact group that has been set up for the follow-up of the implementation of the new standards on VC/VA.
- In the context of the supranational risk assessment report, the Commission will continue to monitor the risks posed by Fin-Tech, crypto-to-crypto currency exchanges and the use of VCs/VAs for the purchase of high-value goods.

13. 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 (sometimes using credit cards in order to legitimise sources of funds). Loans give criminal funds an appearance of legitimacy.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to business loans shows that there have been few cases of terrorist organisations using them as a means of collecting funds. Generally, the organisations do not qualify for such loans (level of salary too low, funds originating from social benefits). In some cases, sanctioned entities (listed organisations) have tried to use business loans to finance terrorist activities through shell companies, but this requires a high level of expertise and knowledge.

Conclusions: There is little evidence that criminals have used/have the intention of using this method. Therefore, the terrorist financing threat related to business loans is considered as less significant (level 1).

Money laundering

The assessment of the money laundering threat related to business loans has found few indications that criminals intend to exploit this risk scenario, which they perceive as unattractive. Most fake loans are a feature of fraud schemes (e.g. two companies take out a fake loan and use a bank to transfer funds); they are not necessarily used to launder the proceeds of crime. Some cases of loans between complicit companies as part of a large scale money laundering system were investigated, but these did not really involve help from the financial sector.

Conclusions: There is little evidence that criminals have used/have the intention of using this method. Therefore, the money laundering threat related to business loans is considered moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of terrorist financing vulnerability related to business loans has been considered in conjunction with money laundering schemes related to business loans.

Conclusions: The level of terrorist financing vulnerability is considered as less significant (level 1).

Money laundering

The assessment of money laundering vulnerability related to business loans made the following findings:

a) risk exposure

The main risk posed by these products lies in their possible early redemption by firms, sometimes in cash (with funds from increasing capital operations of unknown origin).

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. Vulnerability is lower where cash redemption is not accepted. Some conflicts of interest arise where non-performing loans are redeemed.

c) legal framework

Business loans are covered by the AML/CFT framework at EU level. At least in the banking sector, the checks in place are considered to be consistent with the volume of transactions.

Conclusions: The level of money laundering vulnerability is considered moderately significant (level 2).

Mitigating measures

For Member States / competent authorities:

- Thematic inspections of non-bank operators, focusing on the monitoring systems to detect the early redemption of loans.

14. Consumer credit and low-value loans

Product
Credit loan

Sector
Credit and financial sector

Description of the risk scenario

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

Terrorists/organised crime groups use credit cards to withdraw cash from cashpoint machines, generating a negative account balance. They disappear with the funds, with no intention of reimbursing the 'forced' credit.

This kind of loan can also be used to launder the proceeds of criminal activity. The loans are used to buy high value goods (e.g. cars, jewellery) and then redeemed early.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to consumer credit and low value loans shows that terrorist groups use this method to finance travel by foreign terrorist fighters to high risk non EU countries. The most commonly used product is consumer credit. The attraction of low value loans is that they do not necessarily require a high level of expertise or planning. However, greater expertise may be involved where the national legislation requires specific documentation, which some terrorist groups are able to forge.

Conclusions: Consumer credit and low value loans are attractive for terrorist groups, who have used/are using this method quite frequently. Certain jurisdictions may place conditions on access to consumer credit or low value loans, but this does not seem to constitute an obstacle for terrorist organisations. Therefore, the terrorist financing threat related to low value loans is considered significant (level 3).

Money laundering

These products offer less money laundering potential than other financial products, but criminal organisations use them to finance the purchase of high value goods and then redeem the loans by cash.

Conclusions: Consumer credit and low value loans are not as attractive for criminal organisations as other financial products, but they can be used indirectly to launder the proceeds of criminal activity. Transactions are usually low value, but some criminal groups have been able to split large amounts into several transactions. Therefore, the money laundering threat related to low value loans is considered moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of terrorist financing vulnerability related to consumer credit/low-value loans made the following findings:

a) risk exposure

While the products are quite common, they generally involve low amounts, do not attract high risk customers or customers from high-risk countries, and are subject to specific checks by financial institutions. However, the amounts in question can facilitate terrorist action, so the terrorist financing risk exposure is not negligible. The inherent risk can be greater in relation to banking institutions that specialise in fast consumer loans or telecommunications firms offering these products.

b) risk awareness

This assumed low risk exposure is outweighed by the fact that, because of the small amounts, the sector is less aware of the terrorist financing risks. In addition, as with business loans, there is more awareness of risks of fraud than of terrorist financing, so terrorist financing red flags will not necessarily be triggered in the sector. The IT systems in place are not necessarily equipped to detect forged documents. Where financial institutions are involved, the terrorist financing checks can be considered robust, but recent market entrants, such as telecommunications companies, are not subject to AML/CFT obligations, are less aware of the risks and have less effective monitoring systems. Financial intelligence units have noted that suspicious transaction reports are sometimes filed too late, thus virtually ruling out further investigation, as the trail of the possible terrorist will have already gone cold.

c) legal framework and checks

While consumer credit/low-value loans are covered by the AML/CFT framework at EU level, national legislations vary considerably as regards documentation requirements. Some Member States require specific documents, while others do not. Where a loan is granted by a bank, the risks are not necessarily completely mitigated, as funds deposited in a bank account may be withdrawn from an ATM with no checks. New risks can emerge where loans are granted with non-face-to-face identification.

As with other financial products, terrorist financing vulnerability is higher where customers linked to terrorist groups do not appear on sanction lists and therefore do not trigger alerts and red flags in the banking sector. Law enforcement agencies and firms should cooperate more closely to detect potential terrorist financing -risk customers before they perpetrate terrorist acts.

Conclusions: The volume of transactions and amounts at stake are usually low, but that does not reduce the inherent terrorist financing risk. The ineffective alert systems and checks (despite the IT resources in place) adds to the terrorist financing vulnerability. Some new market entrants are less aware of terrorist financing risks than the banking sector. The differences between national legislative frameworks show that the capacity of competent authorities and financial intelligence units to detect suspicious transactions is limited, especially where loans are granted by non-financial entities. Therefore, the level of terrorist financing vulnerability related to low-value loans is considered significant (level 3).

Money laundering

The assessment of money laundering vulnerability related to consumer credit/low-value loans made the following findings:

a) risk exposure

Despite the low amounts, vulnerabilities can be high if firms in the sector do not have proper monitoring systems to detect linked transactions or if customers can redeem loans with cash. The low solvency thresholds to qualify for loans can affect the customer due diligence requirements in the case of financial institutions. The risk is higher where loans come from non-financial institutions not subject to AML/CFT obligations.

Competent authorities have identified risks of fraud deriving from delivery channels that often involve agents whom firms find it hard to monitor. Competent authorities are also concerned about the risk of abuse of credit cards, risks related to money mules and mule accounts, and transfers of funds from cybercrime or online fraud.

b) risk awareness

As with terrorist financing, the assumed low risk exposure is outweighed by the fact that, because of the small amounts, the sector is less aware of the money laundering risks. Again, risk awareness seems more oriented towards risks of fraud than of money laundering. Hence, money laundering red flags are not necessarily triggered in the sector, especially in the event of early redemption. Where financial institutions are involved, money laundering checks can be considered robust, but recent market entrants, such as telecommunications companies, are not subject to AML/CFT obligations, are less aware and have less effective monitoring systems.

c) legal framework and checks

While consumer credit/low-value loans are covered by the AML/CFT framework at EU level, national legislations vary considerably as regards documentation requirements. Some Member States require specific documents, while others do not. Where a loan is granted by a bank, the risks are not necessarily completely mitigated, because funds deposited in a bank account may be withdrawn from a cashpoint machine with no checks. Some additional risk can emerge where new Fin-Tech companies are involved, because of the non-face-to-face customer relationships.

Conclusions: While the volume of transactions and amounts at stake limit the risk exposure of the sector, vulnerability is higher where loans are granted by non-banking institutions. The differences between national legislative frameworks show that the capacity of competent authorities and financial intelligence units to detect suspicious transactions is limited, especially where loans are granted by non-financial entities. Therefore, the level of money laundering vulnerability related to low-value loans is considered moderately significant (level 2).

Mitigating measures

For the Commission:

- Improve cooperation between obliged entities (mainly financial institutions) and law enforcement agencies in order to improve the effectiveness of systems for monitoring terrorist financing.

For Member States / competent authorities:

- Thematic inspections in the sector, focusing on the assessment of monitoring systems to detect the early redemption of loans.

15. Mortgage credit and high-value asset-backed credits

Product
Mortgage credit

Sector
Credit and financial sector

Description of the risk scenario

Money laundering: Perpetrators disguise and invest the proceeds of crime by way of real-estate investment. The proceeds are used for deposits, repayments and early redemption.

Terrorist financing: Perpetrators use (medium/long-term, low-interest) high-value asset-backed credit/mortgage loans to fund plots. Loans are taken out for relatively high amounts to access funds that are untraceable as long as the money is not transferred.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to mortgage credit shows that terrorist groups find this method very difficult to use and to access. In only a few actual cases have terrorist organisations used it to collect funds. It does not correspond to their needs as it requires sophisticated knowledge and technical expertise in the production of complex documentation. In addition, the purpose of mortgage credit is to give a third party access to funds, so it does not give terrorist organisations easy and speedy access to funds unless they have built up a relationship of complicity with such a third party.

Conclusions: Mortgage credit requires a high level of knowledge and expertise to understand the product and provide the relevant documentation (forged documents). It is not attractive, as it involves the complicity of a third party (beneficiary of the funds). Therefore, the terrorist financing threat related to mortgage credit is considered as being of low significance (level 1).

Money laundering

The assessment of the money laundering threat related to mortgage credit shows that organised crime organisations have frequently used this method. They are well equipped to provide false documentation and the structure of the mortgage (with third-party involvement) helps them to hide the real beneficiary of the funds. Mortgage credit constitutes an easy way to enable criminals to own several properties and to hide the true scale of their assets. This method is still used for the integration phase (mostly for lower amounts, as it does not require sophisticated operations). However, it is more often used in combination with concealment of the beneficial owner of real estate behind a complex chain of ownership.

Conclusions: In the money laundering context, mortgage credit is a vehicle favoured by criminal organisations. It enables them to hide the volume of assets and the beneficial ownership. It requires a moderate level of expertise. Consequently, the money laundering threat level related to mortgage credit is considered significant (level 3).

Vulnerability

Terrorist financing

The assessment of terrorist financing vulnerability related to mortgage credit shows that it is not vulnerable to terrorist financing risks — law enforcement agencies have detected few cases (if any). The terrorist financing checks and risk awareness are similar to those for retail banking.

Conclusions: Low significance (level 1)

Money laundering

The assessment of money laundering vulnerability related to mortgage credit shows that:

a) risk exposure

Inherent risk can be high, because of the link with the real-estate sector, which criminal organisations prefer to use to launder the proceeds of their activity by means of high-value transactions. Where credit institutions are involved, inherent risk can be lower, but it is also exposed to high-risk customers (e.g. politically exposed persons) and can involve cross-border transfers of funds.

b) risk awareness

Awareness in credit institutions can be considered high and checks are robust. In addition, other actors in this sector (e.g. notaries) can help to mitigate inherent risk. Nevertheless, banks can face conflicts of interest where laxer checks will allow high-risk customers to redeem large mortgages or non-performing loans.

Vulnerability is higher where real-estate transactions and associated mortgages involve transfers of funds from a bank account in a Member State with weaker anti-money laundering checks for high-risk customers. This weakness is linked to horizontal vulnerabilities in supervision.

There is a good level of reporting, and financial intelligence units and law enforcement agencies are well aware of the vulnerabilities in the sector.

c) legal framework and checks

Mortgage credit is included in the AML/CFT framework at EU level. The checks are considered quite effective where the mortgage credit is provided by credit institutions. In addition, other participants in the process (such as notaries) mitigate the risks.

Conclusions: Where provided by banks, mortgage credit products are as vulnerable as deposits on accounts. The interaction with the real-estate sector generally increases vulnerability, however other participants in the transactions, as notaries, can reduce vulnerability. Therefore, the level of money laundering vulnerability related to mortgage credit is considered moderately significant (level 2).

Mitigating measures

For Member States / competent authorities:

- Thematic inspections in the sector, focusing on the assessment of the monitoring systems to detect the early redemption of loans, and on the effectiveness of customer due diligence measures, especially where High-risk Third Countries customers are involved.

16. 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, with or without guarantees, and include life insurance benefit as a component. Based on the gross written premiums, the most dominant lines of life insurance business in the EEA are unit-linked and index-linked insurance, other life insurance, and with profits insurance.

According to the ECB statistical database, the total reported assets of insurance corporations in the euro area in Q3 2018 were €7.984 billion, of which around €3.305 billion was for life insurance corporations (€1.125 billion for non-life insurance corporations, €579 billion for reinsurance and €2.974 billion for composite insurance corporations).

EU life premiums amounted to €876.2 billion in 2017, according to data published by the European Insurance and Occupational Pensions Authority.

In addition to the AMLD, specific provisions aim to mitigate the risks involved in using life insurance companies as an investment vehicle. Article 59 of Directive 2009/138/EC (Solvency II) (resp. Article 323 of Commission Delegated Regulation (EU) 2015/35) requires an assessment as to whether there are reasonable grounds to suspect that, in connection with the proposed acquisition (resp. qualifying holding of the shareholder or members having a qualifying holding in the special purpose vehicle), money laundering or terrorist financing is being / has been committed or attempted, or that the proposed acquisition (resp. qualifying holding) could increase the risk thereof.

Description of the risk scenario

Perpetrators use fraud involving life-insurance products to fund their activities. Life policies can be redeemed early to generate lump sums, particularly where the proceeds can be transferred.

Money laundering and terrorist financing risks in the insurance industry relate in particular to life insurance and annuity products. These allow a customer to place funds into the financial system and potentially disguise their criminal origin, or to finance illegal activities. Relevant risk scenarios typically involve investment products in life insurance (rather than death benefit products as such).

The risks may arise where:

1. an insurer* accepts a premium payment in cash (this is not a common practice);

2. an insurer refunds premiums, upon policy cancellation or surrender, to an account other than the source of the original funding (owned by a party other than the policyholder);
3. an insurer does not carry out 'know your customer' due diligence in general or establish the source of investments in particular;
4. an insurer sells transferable policies (these 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; and/or
7. an insurer sells a small investment policy initially and the investor makes subsequent large investments without undergoing additional 'know your customer' due diligence.

In scenarios 2, 4 and 6 above, there is a direct and indirect terrorist financing risk.

There is a money laundering risk in all of the above scenarios. Perpetrators use risk scenarios 1, 6 and 7 for placement, 2 and 4 for layering and 2, 4, 6 and 7 for integration.

** All of the above scenarios may involve an insurer, its agent or an intermediary. For the sake of simplicity, we refer to 'insurer'.*

Threat

Terrorist financing

The assessment of the terrorist financing threat related to life insurance shows that terrorist groups have limited interest in this method. It requires specific knowledge of the product and its specific characteristics. Life insurance contracts are not easily accessible and applications require a lot of supporting documentation, which is likely to dissuade terrorist groups. Foreign terrorist fighters may take out life insurance and ask for the funds to be redeemed for the benefit of their family in the event of their suicide or death in battle. However, Member State legislation or insurance companies' underwriting policies often does not allow this type of clause, so the risk is not so great.

Conclusions: Law enforcement agencies have limited evidence of life insurance being misused for terrorist financing purposes. The need for knowledge and planning expertise make this method less attractive. Therefore, the terrorist financing threat related to life insurance is considered moderately significant (level 2).

Money laundering

The assessment of the money laundering threat related to life insurance shows that organised crime organisations can use this method, but complex arrangements are required to hide the proceeds of crime (bank account wrapped in an insurance policy, multiple accounts in third countries loaded with cash and used as collateral for a credit loan, sending money to the life insurance policy). Cases exist, but they are few and sophisticated planning and knowledge are required to make life insurance a viable option.

Conclusions: Some cases of life insurance being abused for money laundering purposes have been detected, but they are generally the result of sophisticated schemes. Therefore, the money laundering threat related to life insurance is considered moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of terrorist financing vulnerability related to life insurance shows that:

a) risk exposure

The misuse of life insurance mostly involves the anonymous placing of funds rather than their withdrawal. However, the risk exposure seems limited, given the volume of transactions concerned. Most competent authorities assess the overall level of inherent terrorist financing risk as being of low or moderate significance. They consider the sector's exposure to the terrorist financing risks arising from cross- border transactions and activities to be insignificant.

b) risk awareness

The sector seems quite unaware of terrorist financing risks. Most suspicious transaction reports are sent quite late in the process, because life insurers tend to wait for funds to be withdrawn before considering whether it is suspicious. Insurers typically have access to much less information about their customers than other sectors (e.g. banks), which reduces their ability to build comprehensive customer risk profiles. The lack of transactions means that suspicious activity is detected mainly on the basis of 'unusual behaviour' and terrorist financing risk is determined at the start of the relationship.

c) legal framework and checks

Life insurance is included in the AML/CFT framework at EU level.

Competent authorities assess the quality of checks in this sector as largely good or very good. Where they identified weaknesses, these related mainly to the quality of both the

business- wide and individual risk assessments, and associated shortcomings in relation to monitoring and the identification and reporting of suspicious transactions.

Conclusions: Risk awareness in the sector is low, with the risk exposure being low as well. There are very few cases due to the limited attractiveness of the product. Therefore, the level of terrorist financing vulnerability related to life insurance is considered as being of low/moderate significance (level 1-2).

Money laundering

The assessment of the money laundering vulnerability related to life insurance shows that:

a) risk exposure

The misuse of life insurance mostly involves the anonymous placing of funds rather than their withdrawal. However, the risk exposure seems rather limited, given the volume of transactions concerned. Most competent authorities assess the overall level of inherent money laundering risk as being of low or moderate significance. They consider the sector's exposure to the money laundering risks arising from cross- border transactions and activities to be insignificant.

b) risk awareness

The sector is well aware of the money laundering risks. However, insurers typically have access to much less information about their customers than other sectors (e.g. banks), which reduces their ability to build up comprehensive customer risk profiles. This lack of transactions means that suspicious activity is detected mainly on the basis of 'unusual behaviour' and money laundering risk is determined at the start of the relationship.

c) legal framework and checks

Services are mostly provided through bank accounts, which are generally covered by effective checks. Competent authorities assess the quality of checks in the sector as largely good or very good. Where they identified weaknesses, these related mainly to the quality of both the business- wide and individual risk assessments, and associated shortcomings in relation to monitoring and the identification and reporting of suspicious transactions.

As in other sectors, Fin-Tech and Reg-Tech solutions are becoming more prevalent in the sector. They are considered an emerging risk by several competent authorities concerned about the lack of awareness (and sometimes the absence) of AML/CTF regulatory requirements applicable to Reg-Tech solutions and Fin-Tech services. A related emerging risk identified by competent authorities is the sector's move to web- based insurance platforms and associated challenges posed by accounts opened without the physical presence of the customer.

Conclusions: Life insurance is currently well framed and the sector seems quite aware of money laundering risks. The checks in place are correctly implemented. Therefore, the level of money laundering vulnerability related to life insurance is considered as being of low/moderate significance (level 1-2). Where life insurance products are used as investment products for wealth management or other investment services, the relevant risk level should be considered.

Mitigating measures

No further proposal is made at this stage.

17. Non-life insurance

Product
Non-life insurance

Sector
Insurance sector

General description of the sector and related product/activity concerned

Non-life insurance policies are generally short-term in nature and serve to provide protection against unexpected loss, such as damage to property. Based on the gross written premiums, the most dominant lines of non-life insurance business are those linked to motor vehicle liability, fire and other damage to property, and medical expenses.

According to the ECB statistical database, the total reported assets of insurance corporations in the euro area for Q3 2018 were €7.984 billion, of which around €1.125 billion was for non-life insurance corporations (€3.305 billion for life insurance corporations, €579 billion for reinsurance and €2,974 billion for composite insurance corporations).

Premiums in the largest non-life insurance market, motor insurance, totalled €137.5 billion in 2017, according to data published by Insurance Europe, followed by those for property insurance (€101.5 billion), accident insurance (€36.1 billion) and general liability insurance (€40.1 billion); health insurance premiums amounted to €131.5 billion.

Specific provisions aim to mitigate the risks involved in holding shares of insurance companies. Article 59 of Directive 2009/138/EC (Solvency II) (resp. Article 323 of Commission Delegated Regulation (EU) 2015/35) requires an assessment as to whether there are reasonable grounds to suspect that, in connection with the proposed acquisition (resp. qualifying holding of the shareholder or members having a qualifying holding in the special purpose vehicle), money laundering or terrorist financing is being / has been committed or attempted, or that the proposed acquisition (resp. qualifying holding) could increase the risk thereof.

Description of the risk scenario

Perpetrators commit fraud involving workplace, car insurance, etc. to fund their activities.

Money laundering can occur in the context of, and as the motive behind, insurance fraud involving non-life insurance, e.g. where this results in a claim to recover part of the invested illegitimate funds. Relevant risk scenarios typically feature high-frequency premiums and cancellations. The risks may arise or materialise where an insurer*:

1. accepts premium payments in cash, although this is not a common practice; or

2. refunds premiums, upon policy cancellation or surrender, to an account other than the source of original funding (owned by a party other than the policyholder).

Money launderers seek to use scenario 1 for placement and scenario 2 for layering/integration.

** In the above examples, the process may involve the insurer or its agent or an intermediary. For the sake of simplicity, we refer to the 'insurer'.*

Threat

Terrorist financing

Similarly, the terrorist financing risk relates to insurance fraud to access sources of revenue for terrorist activities. Such schemes have been detected in workplace insurance and car insurance, for instance. It is difficult to say that this method has no relevance and some evidence of its use has been gathered following terrorist attacks, but it does require a degree of planning and large paper trails that make it relatively unattractive for terrorist groups. However, for the sake of comparison, we can say that it presents the same level of terrorist financing threat as that related to life insurance.

Conclusions: Law enforcement agencies have limited evidence of non-life insurance being misused for terrorist financing purposes. It requires knowledge and planning expertise, which make it relatively unattractive. Therefore, the terrorist financing threat related to non-life insurance is considered moderately significant (level 2).

Money laundering

The assessment of the money laundering threat related to non-life (e.g. car or workplace) insurance shows that, unlike terrorist financing, money laundering abuses require sophisticated schemes that render the risk scenario insufficiently secure or attractive. Law enforcement agencies have no specific evidence of non-life insurance being used to launder the proceeds of crime.

Conclusions: Non-life insurance is not used for money laundering purposes, as it requires a degree of planning and expertise that make it relatively unattractive. Therefore, the money laundering threat related to non-life insurance is considered as being of low significance / no relevance (level 1).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to non-life (e.g. car or workplace) insurance shows that two cases may occur:

(i) undeclared work in motor vehicle retail / car insurance fraud: funds from the fraud are sent by cash transfer; and

(ii) cars are set on fire to obtain the insurance pay-out.

a) risk exposure

The risk exposure is limited, as huge sums of money are concerned and the funds cannot be accessed without prior identification.

b) risk awareness

In general, non-life insurance is more vulnerable than life insurance, because the sector is not necessarily aware of the risks (customer due diligence is not implemented and there is no record-keeping) or specific terrorist financing or money laundering red flags are not always triggered. Insurance issuers tend to pay more attention at the moment of the pay-out, when the risk is perceived to be greater.

c) legal framework and checks

Non-life insurance is not covered by the AML/CFT framework at EU level. Where Member States have regulation in place, checks (in some cases involving self-declarations) seem to work satisfactorily.

Conclusions: In many Member States, legislation has led to checks being carried out and raised awareness in the sector. However, there are still some weaknesses in the detection of suspicious transactions and reporting. Therefore, the level of terrorist financing vulnerability related to non-life insurance is considered moderately significant (level 2).

Money laundering

The assessment of money laundering vulnerability related to non-life (e.g. car or workplace) insurance shows that:

a) risk exposure

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

b) risk awareness

The implementation of customer due diligence is not widespread in the EU, but when Member States have an anti-money laundering framework in place for non-life insurance, they note that obliged entities tend not to apply any customer due diligence at all.

However, considering the number of cases concerned, there is no evidence that this increases the ML risk.

c) legal framework and checks

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

Conclusions: Few cases have been detected of non-life insurance being misused for money laundering purposes. Generally, this is done as part of a broader fraud scheme. Therefore, the level of money laundering vulnerability related to non-life insurance is considered as being of low significance (level 1) / no relevance.

Mitigating measures

No further proposal is made at this stage.

18. Safe custody services

Product
Safe custody services

Sector
Credit and financial sector and private security companies

Description of the risk scenario

Perpetrators rent multiple (commercial or banking) safe custody services to store large amounts of currency, monetary instruments or high-value assets pending their conversion to currency, for placement into the banking system. Similarly, they may establish multiple safe custody accounts to park large amounts of securities pending their sale and conversion into currency, monetary instruments, outgoing funds transfers or a combination of these, for placement into the banking system. Free zones may be used to shelter illicit activities and the proceeds from them.

Threat

Terrorist financing

The terrorist financing threat related to safe custody services is not considered relevant. Therefore, this is not part of the assessment.

Conclusions: Not relevant

Money laundering

The assessment of the money laundering threat related to safe custody services shows that a particular characteristic of this risk scenario is that the assets are stored and not necessarily converted. As a result, it may not be financially attractive. However, it does make it possible to hide the proceeds of crime with no risk of detection. According to law enforcement agencies, these 'dormant' deposit systems are being used increasingly to make safe deposits and take assets out of the financial system.

Exact data are difficult to obtain, because safe custody services are also used for relatives. This is an additional aspect of the money laundering threat, as the person who has deposited funds will not necessarily be the one withdrawing them.

Also, market players other than banks provide such services (storage facilities), which extends the range of tools available to criminal organisations and raises the threat level.

Conclusions: Many Member States have noticed a rising trend in the use of this method by criminal organisations to hide the proceeds of crime. Safe custody services are quite attractive, because they do not require specific expertise and are a fairly secure tool to escape tax or anti-money laundering checks. Therefore, the money laundering threat related to safe deposits is considered significant (level 3).

Vulnerability

Terrorist financing

Terrorist financing vulnerability related to safe custody services is not considered particularly relevant. Therefore, terrorist financing vulnerability is not part of the assessment.

Conclusions: Not relevant.

Money laundering

In assessing the money laundering vulnerability related to safe deposits, a distinction should be made between services provided by credit institutions and those provided by non-banking 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 greater where high-risk customers are involved.

b) risk awareness

Basic aspects of customer due diligence apply to safe custody services provided by credit institutions. Some competent authorities take a proactive approach in this sector, but banks remain vulnerable with regard to the contents of safe deposit boxes. Generally, they have no information on the funds placed in them. The private companies that provide such services do not all comply with AML/CFT requirements and some accept cash payment for the rental of safe deposit boxes. Another question is whether the risk of terrorist financing arises at the time of the storage or only once the funds are inserted in the real economy. From a law enforcement perspective, the more funds are stored, the easier it is to maintain the anonymity of a transaction.

c) legal framework and checks

Safe custody services and free zone 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 providing safe custody services as listed in point 14 in Annex I to Directive 2013/36/EU are specifically subject to AML/CFT rules. However, in practice, financial institutions may not be in a position to meet their monitoring obligations and assess the source of funds, since they are not aware of the contents of the 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: Where provided by credit and financial institutions, safe custody services are subject to customer due diligence requirements and checks. However, it is not always possible to establish the exact source of funds and ongoing monitoring may have a blind spot, since the financial institution is usually unaware of the contents. In addition, safe deposits may be accessible to parties other than the initial customer, which increases vulnerability. The market is fragmented, with the emergence of private entities and other commercial storage/safe services. Therefore, the level of money laundering vulnerability is considered moderately significant/significant (level 2-3).

Mitigating measures

For Member States / competent authorities:

- Thematic inspections in the sector, focusing on the effectiveness of customer due diligence requirements of financial and non-financial institutions offering safe custody services.

1. Creation of legal entities and legal arrangements

Product/Service
Creation of legal entities and legal arrangements

Sector
Trust or company service providers (TCSPs), legal professionals, tax advisors/accountants/auditors, providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice ('professional intermediaries')

General description of the sector and the related product/activity concerned

TCSPs, legal professionals, tax advisors/accountants and providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice provide a wide range of services to individuals and businesses for commercial undertakings and wealth management.

The Fourth Anti-Money Laundering Directive (4th AMLD) requires entities to identify the beneficial owner when entering into a business relationship and to take risk-based and adequate measures to verify the identity of the beneficial owners as defined in Article 3(6).

In addition to anti-money laundering 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. European company law is partially codified in Directive 2017/1132/EU[49] relating to certain aspects of company law, and Member States continue to operate separate company acts, which are amended from time to time to comply with EU directives and regulations.

Directive 2017/1132/EU covers:

1. 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.
2. 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 €25,000.

3. 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.

Additionally, Directive 2009/102/EC[50] on company law on single-member private limited liability companies 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 12th Council Company Law Directive).

- This Directive also 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.**[51]

Listed companies must also meet certain **transparency requirements.**[52]

Description of the risk scenario

Perpetrators create complex structures involving many jurisdictions, in particular offshore jurisdictions with secretive chains of ownership, normally through shell companies,[53] 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 creating 'opaque structures', which are defined as structures where the true identity of the UBO(s) of entities and arrangements in that structure is concealed, for example, through the use of nominee directors for instance. In such cases, it is only the nominee director who appears to be the beneficial owner of the company. These schemes make use of offshore jurisdictions with weak ML/TF frameworks which attract significant investments. The amount of global offshore wealth held in 2017 was around

[50] Directive 2009/102/EC of the European Parliament and of the Council of 16 September 2009 in the area of company law on single-member private limited liability companies (Text with EEA relevance); OJ L 258, 1.10.2009, p. 20-25.
[51] Company reporting: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[52] Securities markets: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.
[53] An overview of shell companies in the European Union: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/627129/EPRS_STU(2018)627129_EN.pdf.

$8.2 trillion, 6% higher than in the previous year in US dollar terms.[54] A preliminary estimate of offshore wealth held by EU residents is e $1.6 trillion in 2016.[55]

General comment

For this risk scenario, the assessment covers legal entities such as companies, corporate structures, foundations, associations, not-for-profit organisations, charities and similar structures. It also covers trusts and other legal arrangements with a similar structure or function (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 do not have a legal personality and are basically a contractual relationship). However, as far as the nature of the service is concerned (here the creation of the structure), these specific features do not make any key difference: legal entities and legal arrangements can be used in the same way for hiding the true beneficial owners. The type of structure perpetrators favour depends on the legal environment of a given jurisdiction, the perpetrators' type of expertise and convenience. Organised crime groups can easily create all of these structures and all of them could be vehicles for creating opaque and complex schemes that make it more difficult to identify the real owner and the real origin of the funds.

Threat

Terrorist financing

Perpetrators intend to set up opaque structures that can circumvent any restrictive measures in place. The assessment of the terrorist financing threat related to the creation of legal entities and legal arrangements shows that terrorist organisations may have difficulty in creating such structures. This is because these terrorist organisations are usually on the 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 only be provided by professional intermediaries. Nevertheless, law enforcement agencies and financial intelligence units have identified some simple methods that involve perpetrators using bank accounts and professional intermediaries to help them set up structures quickly and easily in order to gather cash to finance terrorist activities. Therefore, the ability to create legal entities and legal arrangements is relevant for the terrorist financing threat, although only a limited number of such cases have been reported by law enforcement.

Conclusions: Few cases of using these methods to finance terrorism have been identified. This may be because the high level of technical expertise and knowledge required dissuades terrorist organisations that would prefer simpler and more

[54] Global Wealth 2018 report by The Boston Consulting Group: http://image-src.bcg.com/Images/BCG-Seizing-the-Analytics-Advantage-June-2018-R-3_tcm9-194512.pdf.
[55] Forthcoming study by ECOPA and CASE: *'Estimating International Tax Evasion by Individuals'.*

accessible solutions. Therefore, the level of terrorist financing threat related to the creation of legal structures is considered as moderately significant (level 2).

Money laundering

The assessment of the money laundering threat related to the creation of legal entities and legal arrangements shows that this tool is almost exclusively used to hide and obscure the beneficial ownership. From a costs perspective, setting up a legal entity or a legal arrangement is rather straightforward and can be done online. Shell companies with a generic declared activity and no operations are very common. Shell companies that have already been in operation for a few years whose shares are transferred to new shareholders are more expensive but also more sought after by criminals. Foundations are also attractive as no control on funds is carried out by competent authorities. All such entities lack real economic activities. Some costs or a 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 jurisdiction 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. Complex chains of ownership throughout different countries increase the opacity of the money laundering scheme. However, on the creation of the structure itself, as long as the use of intermediaries is sufficient to hide the beneficial ownership, it is an attractive and fairly secure method to launder the proceeds of crime.

Financial intelligence units and law enforcement agencies consider that criminal organisations use this method frequently. One organised criminal group can use several types of professional enablers depending on the task. This has been a key feature in most of the cases reported to Europol, where money laundering schemes are facilitated by professionals from different industries, usually a lawyer and an accountant. For example, economic advisors are used to design a mechanism to integrate criminal cash into the legal financial system, and lawyers find a legal justification for these activities. This accounts for the complexity of the laundering mechanisms in place and the need for expert knowledge to build them and avoid detection.

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

Vulnerability

Terrorist financing

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

a) risk exposure

The risk exposure aspect is 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). 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-to-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 terrorist financing schemes.

b) risk awareness

In general, professional intermediaries seem to be aware of 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 terrorist financing 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 providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice (since 2005) are subject to EU anti-money laundering requirements.

Based on the level of suspicious transaction reporting, competent authorities consider that the checks in place are still insufficient and the elements gathered at the beginning of the business relationships are not developed enough to detect and analyse the terrorist financing risks related to the creation of legal entities or legal arrangements.

EU Member States have different regulatory and taxation regimes that may be exploited by terrorist organisations. Enforcing the requirements on the identification of the beneficial owner at the beginning of the business relationship remains an important challenge for the entities concerned. Although it is difficult to link shell companies to their owners, security experts and law enforcement officials all agree that shell companies, or other legal entities like trusts, pose a threat to national security. They make it nearly impossible to find the people who are actually financing terrorism and other criminal activities, and can be ideal vehicles for financing terrorists.[56]

On providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice, there is no information about how

[56] 'These U.S. companies hide drug dealers, mobsters and terrorists', Melanie Hicken and Blake Ellis, CNN Money, 9 December 2015.

they are supervised by the competent authorities and whether or not they comply with anti-money laundering and terrorist financing requirements.

Conclusions: Although this is not necessarily the most frequent method used for terrorist financing, the terrorist financing vulnerability related to the creation of legal structures is considered as significant/very significant (level 3/4).

Money laundering

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

a) risk exposure

The main risk exposure aspect is 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). 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-to-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 money laundering schemes.

b) risk awareness

Both TCSPs and legal professions/tax advisors seem to be aware of 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 significant shortcomings in enforcement. This is the case when several obliged entities are involved in the creation of structures and where the application of customer due diligence, 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 significant shortcomings in entities' understanding of their anti-money laundering obligations or even knowledge of these obligations. This particularly applies to the use of common law legal arrangements, like trusts, which are less transparent legal structures that are unfamiliar to civil law countries and are not known in their national law or used as investments/business vehicles. Even when guidance on how to apply anti-money laundering requirements to legal arrangements in these civil law jurisdictions — and the applicability of CDD — is available, getting an orderly view of these legal structures remains difficult. This is especially the case for common law legal agreements made in non-EU countries.

The risk awareness of providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice is impossible to assess as there is no information available on 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 providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice (since 2005) are subject to EU anti-money laundering requirements.

The current EU legal framework requires: (i) the identification of the beneficial owner before entering into a business relationship; and (ii) that Member States establish a central register on the beneficial ownership of corporate and other legal entities incorporated within each Member State's territory.

Nevertheless EU Member States still have different regulatory and taxation regimes that are exploited by criminal organisations. These organisations may take advantage of more lenient AML/CFT frameworks to identify beneficial owners of legal entities and arrangements or of national regimes that do not provide for personal or corporate income tax.

Controls: Competent authorities and financial intelligence units have noticed the involvement of offshore jurisdictions where the ability of law enforcement agencies to conduct investigations depends on the existence of mutual legal assistance (MLA) agreements with these jurisdictions. The consequence is that if there is no MLA agreement, the process to identify the beneficial ownership is hampered.

IT tools have been put in place to allow corporate structures to be created quickly and anonymously without the involvement of a public authority. In the case of legal arrangements, some of them can be contracted in a very informal way which creates additional obstacles for carrying out inspections.

On providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice, there is no information on how competent authorities supervise them and whether or not they comply with AML/CFT requirements.

Conclusions: The money laundering risk exposure relating to the creation of legal entities or legal arrangements is considered to be significant due to the still existing level of anonymity and the characteristics of the customers and areas involved, in particular when basic or simplified IT tools are being used without the involvement of a public authority. The risk awareness of professional intermediaries seems quite satisfactory although the number of STRs remains very low[57].

[57] The 2013 FATF report notes that '*the level of reporting by the legal sector is unlikely to be at the same level as that of the financial institutions. There is a significant difference in the volume of transactions*

Even after Member States' transposition of EU AML Directives and the designation of designated non-financial businesses and professions since 2001 many Member States still lack a robust AML/CFT framework in many Member States and the rules do not seem to be correctly understood. The legal framework is not adapted to the risk (beneficial ownership is identified after the creation of the structure rather than before) and the necessary checks were introduced only recently with the 4th and 5th AML Directives. Therefore, the money laundering vulnerability related to the creation of legal entities, legal arrangements and non-profit organisations/charities is considered as significant/very significant (level 3/4).

Mitigating measures

While there have been significant improvements in the adoption and implementation of Financial Action Task Force (FATF) standards and Member States' endorsement of the Organisation for Economic Cooperation and Development's work on transparency in recent years, the need to further increase the overall transparency of the EU's economic and financial environment is clear. We cannot prevent money laundering and terrorist financing effectively unless the environment is hostile to criminals seeking shelter for their finances through non-transparent structures. The integrity of the EU financial system depends on the transparency of corporate and other legal entities, trusts and similar legal arrangements. The overarching principles of EU action are to detect and investigate money laundering and to prevent it from occurring. Increasing transparency could be a powerful deterrent.

Since the preparation of the first Supranational Risk Assessment (SNRA) report, the EU has revised its AML/CTF legal framework to mitigate risks relating to money laundering and terrorist financing. In 2015, the EU adopted a modernised regulatory framework encompassing:

- **Directive (EU) 2015/849** on preventing the use of the financial system for money laundering or terrorist financing (4th AMLD).[58]
- **Regulation (EU) 2015/847** on information on the payer accompanying transfers of funds[59] — makes fund transfers more transparent, thereby helping law enforcement authorities to track down terrorists and criminals.

---

undertaken by legal professionals in comparison to financial institutions. Also, the level of involvement in each transaction, which affects the basis on which a suspicion may arise and be assessed, is significantly different.' Accordingly, the report identifies, on page 24, *'a more relevant comparison'* for the legal sector as perhaps being with other DFNBPs *'especially those providing professional services'* from which *'reports by legal professionals averaged 10 %, ranging from less than 1 % to 20 %'*. The report includes a sampling of STRs for legal professionals and DNFBPs in 2010 and 2011 for a number of countries.

[58] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance); OJ L 141, 5.6.2015, p. 73-117.

Both pieces of legislation take the FATC's 2012 recommendations into account and go further on a number of issues to promote the highest possible anti-money laundering standards and to counter terrorist financing.

- **Directive (EU) 2018/843, the 5th AMLD**[60] **(Amendments to the 4th AMLD).**
- **Directive 2018/822/EU**[61] which requires intermediaries to submit information on reportable cross-border tax arrangements to their national authorities[62] comes into effect as from 2020.

The 5th AMLD, which amends the 4th AMLD was published in the Official Journal of the European Union on 19 June 2018. The Member States must transpose this Directive by 10 January 2020, but certain changes need to be implemented by 10 March 2020. The interconnection of the registers on beneficial ownership is required by 10 March 2021.

On the creation of legal entities and legal arrangements specifically, the amendments introduced by this new legal framework:

- improve transparency on the real owners of companies;
- improve transparency on the real owners of trusts;
- establish the interconnection of the beneficial ownership registers at EU level; and
- improve cooperation and information sharing between anti-money laundering supervisors and between them and prudential supervisors and the European Central Bank.

Within this improved framework, the main tasks for competent authorities/self-regulatory bodies remain:

- Member States should ensure that competent authorities/self-regulatory bodies provide training sessions and guidance on risk factors with a focus on non-face-

[59] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Text with EEA relevance); OJ L 141, 5.6.2015, p. 1-18.
[60] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 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 Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance); OJ L 156, 19.6.2018, p. 43-74.
[61] Council Directive (EU) 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements; OJ L 139, 5.6.2018, p. 1-13.
[62] Administrative cooperation in (direct) taxation in the EU: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

to-face business relationships, offshore professional intermediaries, customers or jurisdictions and complex/shell structures.

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

- Annual reports on the measures taken to verify these entities' compliance with their customer due diligence obligations, 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 ensure that providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice comply with their obligations on beneficial ownership.

2. 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 advice on capital structure, industrial strategy and related questions and advice and services for mergers and purchasing undertakings ('professional intermediaries')

General description of the sector and the related product/activity concerned

TCSPs, legal professionals, tax advisors/accountants and providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice provide a wide range of services to individuals and businesses for commercial undertakings and wealth management.

The 4th AMLD requires obliged entities to 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 anti-money laundering legislation, the following EU company law directives lay down general rules on setting up limited liability companies, especially on capital and disclosure requirements. EU company law is partially codified in Directive 2017/1132/EU relating to certain aspects of company law, and Member States continue to operate separate company acts, which are amended from time to time to comply with EU directives and regulations.

Directive 2017/1132/EU covers:

1. 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.
2. 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 €25,000.

3. 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.

Additionally, **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.**[63]

Listed companies must also meet certain **transparency requirements.**[64]

Description of the risk scenario

Front companies used for fraud via false invoicing: Perpetrators use front companies 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) to justify the movement of criminal proceeds through banking channels (via letters of credit, invoices, etc.) or through the use of global transactions, often using false documents for the trade of goods and services[65]. 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[66].

False loans: Companies set up fictitious loans with each other to create an information trail to justify transfers of funds of illegal origin. Perpetrators use fictitious loans to justify the movement of criminal proceeds through banking channels — without any economic backing.

In terms of legislation, the EU has adopted several accounting directives[67] and has set audit requirements to ensure that companies' accounts represent a true and fair view.

General comment

---

[63] Company reporting:
https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[64] Securities markets:
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.
[65] Trade-Based Money Laundering — by FATF:
http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html.
[66] '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.
[67] Company reporting overview:
https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en#overview.

For this risk scenario, the assessment covers legal entities such as companies, corporate structures, foundations, associations, not-for-profit organisations, charities and similar structures. It also covers trusts or other legal arrangements with 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 do not have a legal personality and are basically a contractual relationship). However, as far as the nature of the service is concerned (here the creation of the structure), these specific characteristics do not make any key difference: legal entities and legal arrangements can be used the same way for hiding the true beneficial owners. The type of structure perpetrators favour depends on the legal environment of a given jurisdiction, the perpetrators' type of expertise and convenience. Organised crime groups can easily create all of these structures and all of them could be vehicles for creating opaque and complex schemes that make it more difficult to identify the real owner and the real origin of the funds.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to business activities of legal entities or legal arrangements shows that terrorists groups do not particularly favour this kind of method to finance terrorist activities. According to law enforcement authorities, this risk scenario is not really attractive for terrorists groups as it requires the creation of an opaque structure (illicit legal entity or legal arrangement) or infiltrating the ownership of a legitimate legal entity or legal arrangement. It requires expertise and the ability to plan. Due to the different steps to be taken, it is unlikely that 'clean' money can be collected quickly from this method. However if perpetrators have the expertise, they can use this method for money remittance instead of other classical techniques (money value transfer services, hawala, etc.). The method can be attractive if there is a need to transfer large volume of funds for terrorist financing purposes. Therefore, terrorist groups may have some intentions to use it.

Conclusions: From the evidence provided by law enforcement authorities and financial intelligence units, the level of the terrorist financing threat related to business activities of legal entities and legal arrangements is considered as <u>moderately significant</u> (level 2).

<u>Money laundering</u>

The assessment of the money laundering threat related to business activities of legal entities or legal arrangements shows that the most widespread means used by organised crime groups to launder the proceeds of crime are TBML 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; and (iv) by laundering illegitimate proceeds by withdrawing cash from another company's account using intermediaries. More and more trade operations are actually legal and involve the export of goods and commodities at a market price, but mostly paid in cash and exported before being re-exported between different countries. It mainly involves high value goods (cars,

electronics goods, luxury goods), but it increasingly includes low value/large volume goods such as agrofood goods.

In virtually all cases, organised crime groups use legal business structures to launder their criminal proceeds. This is commonly known as business recycling. Cash-intensive businesses such as catering or retail provide a good cover for the source of otherwise inexplicable quantities of cash. These businesses can be exploited in a variety of ways by OCGs, but in most cases they are used as a legitimate source of income from customers to facilitate the co-mingling of illicit funds with legal proceeds. In these cases the services of a complicit bookkeeper or accountant are used in order to legitimise criminal cash flows through false invoices, receipts and accounts. In some other cases, the business does not have any legitimate activity, and therefore no legitimate source of cash. Fictitious accounts and transactions are therefore created in order to disguise criminal proceeds as legitimate earnings of trade in goods and services. Financial statements can also be falsified to account for the cash flows.

While the required expertise and planning capacity is not negligible, law enforcement authorities and financial intelligence units consider that OCGs have used this method frequently because it is generally quite accessible, has a low cost and is relatively easy to exploit. However, this method also involves several sectors. For example, transfers of money through companies' structures are generally processed through the banking sector.

Conclusions: While building a TBML scheme may require moderate levels of technical expertise and knowledge, financial intelligence units and law enforcement agencies have identified many such cases that demonstrate that this method is quite easy to access and to exploit. On this basis, the level of the money laundering threat related to business activities of legal entities and legal arrangements and based on trade-based money laundering is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing 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 mostly 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 of the risk of being misused to create legal entities and legal arrangements for illegitimate purposes linked to money laundering and terrorist financing. The risk that these structures could be used to hide the beneficial owner is well known. However, there are still significant shortcomings in their understanding of their AML/CFT obligations, or even their knowledge of them. In particular, given that in the context of terrorist financing business

activity can still rely on legitimate money, this does not necessarily trigger any red flags. The checks in place are quite weak, so financial intelligence units can only detect and analyse the terrorist financing risks related to business activity through legal entities or legal arrangements 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 checks

Legal framework: Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice (since 2005) are subject to 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.

Checks:
Competent authorities consider that there are still not enough checks in place and that elements gathered at the beginning of business relationships are not sufficient to detect and analyse the terrorist financing risks related to the creation and activities of legal entities and legal arrangements.

Regarding providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice, there is no information about their supervision by competent authorities and whether or not they comply with AML/CFT requirements.

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

Money laundering

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

a) risk exposure

False loans are used widely by organised crime groups. In certain cases, TBML 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 of the risk of being misused to create legal entities and legal arrangements for illegitimate purposes linked to

money laundering and terrorist financing. 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 the investigation work of law enforcement agencies harder. The illicit origin of the funds is generally difficult to prove due to the number of people/bodies and geographical areas involved and the channels used. Suspicious transactions are therefore quite difficult to detect (TBML and false invoicing).

c) legal framework and checks

Legal framework: Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice (since 2005) are subject to 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.

Checks: in several situations, competent authorities and financial intelligence units have noticed the involvement of offshore jurisdictions where the ability of law enforcement agencies 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.

For providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice, there is no information on their supervision by competent authorities and whether or not they comply with AML/CFT requirements.

Conclusion: The risk exposure of the sector is considered to be very significant due to the lack of a robust money laundering framework in many non-EU country jurisdictions, especially the lack of rules on identifying beneficial owners. This means that checks are non-existent 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 money laundering vulnerability related to business activities through a legal structure and based on TBML is considered as significant/very significant (level 3/4).

Mitigating measures

Under the improved legal framework introduced by the 4th AMLD and the amendments provided by the 5th AMLD transparency requirements for beneficial ownership information on legal entities and legal arrangements have been reinforced:

- The specific factor determining which Member State is responsible for the monitoring and registration of beneficial ownership information of trusts and similar legal arrangements has been clarified.

- Public access to beneficial ownership information allows greater scrutiny of information by civil society, including by the press or civil society organisations, and contributes to preserving trust in the integrity of business transactions and of the financial system.

- The strengthened public scrutiny helps prevent the misuse of legal entities and legal arrangements, including tax avoidance.

- Member States' central registers holding beneficial ownership information will be interconnected through the European Central Platform established by Directive (EU) 2017/1132.

- Directive 2018/822/EU comes into effect as from 2020 where intermediaries are required to report to their national authorities automatic exchange of reportable information on reportable cross-border tax arrangements.[68]

Within this improved framework, the main tasks for competent authorities/self-regulatory bodies remain:

- Competent authorities/self-regulatory bodies should provide training sessions and guidance on risk factors with a focus on non-face-to-face business relationships, offshore professional intermediaries or customers or jurisdictions and 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 taken to verify these entities' compliance with their customer due diligence obligations, including beneficial ownership requirements, suspicious transaction reports and internal controls, should be provided by competent authorities/self-regulatory bodies to Member States.

[68] Administrative cooperation in (direct) taxation in the EU: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

3. Termination of legal entities and legal arrangements

Product
Termination of business activity of legal entities and legal arrangements

Sector
Trust or company service providers (TCSPs), legal professionals, tax advisors/accountants/auditors, providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice ('professional intermediaries')

General description of the sector and the related product/activity concerned

TCSPs, legal professionals, tax advisors/accountants and providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice provide a wide range of services to individuals and businesses for commercial undertakings and wealth management.

The 4th AMLD requires certain entities to 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 anti-money laundering 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. European company law is partially codified in Directive 2017/1132/EU[69] relating to certain aspects of company law, and Member States continue to operate separate company acts, which are amended from time to time to comply with EU directives and regulations.

Directive 2017/1132/EU covers:

[69] Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (Text with EEA relevance); OJ L 169, 30.6.2017, p. 46-127.

1. 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.
2. 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 €25,000.
3. 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.

Additionally, **Directive 2009/102/EC**[70] (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.**[71]

Listed companies must also meet certain **transparency requirements.**[72]

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 but now without financial difficulties. Perpetrators cash out funds from the front company before the illegal activities are detected or before assets are seized by competent authorities, masking the audit trail of money laundered through the liquidated company.

General comment

For this risk scenario, the assessment covers legal entities such as companies, corporate structures, foundations, associations, not-for-profit organisations, charities and similar structures. It also covers trusts or other legal arrangements with 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 do not have a legal personality and are basically a contractual relationship). However, as far as the nature of the service is concerned (here the creation of the structure), these specific features do not make any key difference: legal entities and legal

[70] Directive 2009/102/EC of the European Parliament and of the Council of 16 September 2009 in the area of company law on single-member private limited liability companies (Text with EEA relevance); OJ L 258, 1.10.2009, p. 20-25.
[71] Company reporting:
https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting_en.
[72] Securities markets:
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets_en.

arrangements can be used the same way for hiding the true beneficial owners. The type of structure perpetrators favour depends on the legal environment of a given jurisdiction, the perpetrators' type of expertise and convenience. Organised crime groups can easily create all of these structures and all of them could be vehicles for creating opaque and complex schemes that make it more difficult to identify the real owner and the real origin of the funds.

Threat

Terrorist financing

The assessment of the terrorist financing threat posed by the termination of business activity has been considered together with money laundering schemes related to the termination of business activity in order to hide the illegal origin of the funds. In such situations, the terrorist financing threat is not lessened with a separate assessment.

Conclusion: The assessment of the terrorist financing threat posed by the termination of activities is considered as slightly/moderately significant (level 1/2).

Money laundering

The assessment of the money laundering threat posed by 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 method as unattractive or difficult to access as it requires some logistical and planning capabilities.

Conclusions: From the elements gathered during the assessment phase, the level of the money laundering threat posed by the termination of business activity is considered as slightly/moderately significant (level 1/2).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerabilities posed by the termination of business activity has been considered together with money laundering schemes related to termination of business activity in order to hide the illegal origin of the funds. In such situations, the terrorist financing threat is not lessened with a separate assessment.

Conclusions: In such situations, the level of vulnerability is moderately significant (level 2)

Money laundering

The assessment of the money laundering vulnerability posed by the termination of business activity through legal structures shows that:

a) risk exposure

Situations where the termination of a business activity is at stake generally starts from a fraud incident.

b) risk awareness

The detection of this method by law enforcement agencies and financial intelligence units is easy given that it mostly starts from a fraud incident. This predicate offence triggers the red flags for either the sector or the competent authorities. In general, bankruptcy is complex to realise and obliged entities (banks in particular) pay particular attention to such scenarios, most of which are considered to be suspicious.

c) legal framework and controls

Accountants, auditors, tax advisors and legal professionals (since 2001), TCSPs (since 2005) and providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice (since 2005) are subject to EU anti-money laundering requirements.

There is no specific provision that covers this situation in the EU anti-money laundering framework, apart from obliged entities being required to identify and report suspicions obligations. But the number of suspicious transaction reports received tends to show that the checks in place are efficient and allow the detection of the suspicion situations. Insolvency Directors managing an insolvency procedure are also an additional control element.

For providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice, there is no information on their supervision by competent authorities and on whether 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, leads to the assessment that the level of vulnerability is moderately significant (level 2).

Mitigating measures

The current EU legal framework has reinforced the transparency requirements for beneficial ownership information on legal entities and legal arrangements. It has also specified and clarified the role of certain parties as obliged entities.

Within this improved framework, the main tasks for competent authorities/self-regulatory bodies remain:

A/ if the termination is related to the creation of another legal entity or legal arrangements

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 a focus on non-face-to-face business relationships, offshore professional intermediaries or customers or jurisdictions, and 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 taken to verify compliance by these obliged entities with their customer due diligence obligations, 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 the supervision of a professional (obliged entity), who should have to develop their due diligence.

- Member States should put in place mechanisms to ensure that the information held in the central beneficial ownership register is verified regularly.

- Member States should ensure that providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice comply with their obligations on beneficial ownership.

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

For competent authorities/self-regulatory bodies:

- Competent authorities/self-regulatory bodies should provide training sessions and guidance on risk factors with a focus on non-face-to-face business relationships, offshore professional intermediaries or customers or jurisdictions, and 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 taken to verify compliance by these obliged entities with their customer due diligence obligations, including beneficial ownership requirements, suspicious transaction reports and internal controls.

- Member States should put in place mechanisms to ensure that the information held in the central beneficial ownership register is verified regularly.

Member States should ensure that providers of advice on capital structure and industrial strategy, advice and services on mergers and acquisitions and business strategy advice are properly regulated and supervised at national level and comply with their obligations on beneficial ownership.

4. 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 trade categories, estimated at possibly the third or fourth largest category. However there are hardly any instruments for measuring the legal trade or any data on the magnitude of the illicit commerce (the specific feature of this illicit trade being that the legal and the illicit trade are sometimes interwoven).

There are hardly any data or instruments for measuring illicit commerce. Nevertheless, according to Interpol, the black market in works of art is becoming as lucrative as those for drugs, weapons and counterfeit goods.

The information dossier that UNESCO produced for the 40th anniversary of the 1970 Convention states that, together with the drugs and armaments trades, the black market in antiquities and culture constitutes one of the most firmly rooted illicit trades in the world[73].

The value of the illegal antiquities traffic is also hard to assess[74] due to its invisible and seamless character.[75] It is estimated that only 30-40 % of antique dealings take place

[73] UNESCO. The Fight against the Illicit Trafficking of Cultural Objects: the 1970 Convention: Past and Future. 15 and 16 March 2011. http://unesdoc.unesco.org/images/0019/001916/191606E.pdf.
[74] Alesia Koush 'Fight against the Illegal Antiquities' Traffic in the EU: Bridging the Legislative Gaps' Bruges, College of Europe 2011; Hardy 'Illicit trafficking, provenance research and due diligence: the state of the art'. Research study, 30 March 2016.

through auction houses where the pieces are published in catalogues.[76] The rest occurs through private (thus often unmonitored, and not recorded) transactions.[77]

According to studies, the total financial value of the illegal antiquities and art trade is larger than any other area of international crime except for arms trafficking and narcotics[78] and has been estimated at $3-6 billion per year.[79]

Links between the antiquities trade and drug, wildlife and arms trafficking, money laundering and tax evasion and the financing of war machines and terror organisations have been widely reported, which puts antiquities trafficking on the level of serious transnational organised crime.

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 terrorist financing threat posed by the trafficking of looted artefacts and antiques shows that law enforcement agencies have identified cases of trafficking of looted antiquities within the EU. Several investigations have been conducted by Member States' law enforcement agencies where underlying trafficking in goods taken out of conflict zones[80] via involvement of far east countries was used to hide more easily the provenance of goods. The share of the illegal market should, of course, be considered but is by definition difficult to detect. From the 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 the terrorist organisations that control the territory then imposing taxes on these activities. For example, 'rather than trading artefacts, Islamic State is earning money from selling digging permits and charging transit fees'.[81] However, terrorists may also sell the products themselves to obtain revenues, as shown by primary evidence collected by the U.S.[82] and as acknowledged by the United Nations Security Council.[83]

---

[75] Duncan Chappell & Kenneth Polk, Unravelling the Cordata‖: Just How Organised Is the International Traffic in Cultural Objects?', in Stefano Manacorda & Duncan Chappell (eds.), *Crime in the Art and Antiquities' World. Illegal Trafficking in Cultural Property.*

[76] Peter Watson, Sotheby's: The Inside Story, Random House, 1997, cited in Chauncey D. Steele.

[77] Alesia Koush, op. cit., p. 4.

[78] Lisa J. Borodkin, The Economics of Antiquities looting and a Proposed Legal Alternative', *Columbia Law Review*, No 2, 1995, p. 377-418.

[79] *Ibid.,* p. 377. Estimation by the author.

[80] https://blogs.state.gov/stories/2018/06/20/en/tackling-illicit-trafficking-antiquities-and-its-ties-terrorist-financing

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

[82] https://www.justice.gov/usao-dc/pr/united-states-files-complaint-seeking-forfeiture-antiquities-associated-islamic-state

[83] UNSC Resolution 2347(2017) recognises (like R 2199, adopted under the binding Chapter VII) that the Islamic State and groups associated with Al Qaeda are 'generating income from engaging directly or indirectly in the looting and smuggling of cultural heritage' using it to fund *'recruitment efforts and strengthen their operational capability to organise and carry out terrorist attacks'.*

The majority of the objects stolen by terrorists in some conflict areas are small/medium size items which come from illegal excavations, making it even harder for the law enforcement agencies to establish the provenance and to prove that a certificate is fake, especially for small items.

Since the products might be sold in the EU by intermediaries, there is an indirect though concrete 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 generate a substantial amount of revenue. However, it is not an easy method. It requires (in the source countries): access to the illegal/dark economy (the items being then often laundered and mixed with legal circuits in the destination countries); technical expertise; and knowledge of the art market, which is not in all terrorist groups' capability. Furthermore, transporting such products is not secure or discrete enough and converting them into case requires time to plan, which is not consistent with terrorist groups' needs to access cash quickly.

The international dimension of this threat cannot be excluded from the threat analysis. Law enforcement authorities and the UN have reported evidence that artefact looting and trafficking occurs in conflict zones. Such activities produce financial revenues that can be used by returning foreign terrorist fighters to commit terrorist acts in the EU territory. There is also evidence of some radicalised people in the EU having been found in possession of unprovenanced artefacts.

Conclusion: At this stage, there is limited evidence that the trafficking of looted artefacts and antiques would be specifically used to finance terrorist activities in the EU. However, it is an attractive source of revenue for organisations controlling territory in conflict zones that intend to finance terrorist activities in the EU. Nevertheless, the level of knowledge, expertise and planning capabilities required reduces the level of threat. The level of terrorist financing threat related to the trafficking of artefacts and antiques is therefore considered as <u>moderately significant</u> (though increased due to the situation in the Middle East and North Africa, and the fact that the disappearance of the territorial 'Caliphate' — which had institutionalised the looting — does not stop the continuation of some low-scale looting) (level 2).

Money laundering

The assessment of the money laundering threat posed by the trafficking of looted artefacts and antiques shows that this risk scenario may be interesting to organised crime groups, as these 'products' can be converted into cash to launder the proceeds of crime or evade tax. Law enforcement agencies consider that this kind of traffic occurs mostly in freeport zones and that this makes it more difficult to measure the extent of the phenomenon. There is evidence that organised crime groups use this method (for which expertise and knowledge is needed to sell the goods at the best price). The illegal economy also plays a role in this risk scenario but is, by definition, difficult to assess. Some criminal networks have attempted to pass off counterfeit goods as stolen pillaged antiquities and have provided fraudulent provenance of the items.

Conclusions: This risk scenario may be an attractive tool for organised crime groups to convert the proceeds of crime in clean cash. However, it requires high

level of expertise and is not a secure activity for them. The level of money laundering threat related to the trafficking of artefacts and antiques is therefore considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability posed by the trafficking of looted artefacts and antiques shows that this risk is currently only an emerging but that it may increase in the short term. Looted goods may be repatriated to the EU in the current climate. For example, some small stolen artefacts/coins may be sold by home grown radicalised people returning to the EU in quantities that are possibly too small to be detected or even prosecuted.

a) risk exposure

Investigations show that antiquities are offered to EU collectors from various non-EU countries, generally through internet auction sites or specialised 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 amounts) but online transactions are also widespread with no possibility for the financial institution to identify to real owner/buyer of the antiquities. There is no specific monitoring of the transactions.

b) risk awareness

According to law enforcement agencies, cultural artefacts either do not arrive on EU territory or remain undetected. This tends to demonstrate that competent authorities and financial intelligence units visibility in this matter is very low. Obliged entities do not carry out any record keeping (e.g. on the origin of artefacts or to whom they are sold) and there is no reporting. Customs authorities have difficulties detecting the illicit origin of cultural artefacts.

c) legal framework and controls

AML framework: under the EU's current anti-money laundering framework, individuals trading in goods are subject to relevant EU requirements when they receive payments in cash of an amount of €10,000 or more. This requirement focuses on payments in cash and does not consider risks of other types of payment transactions.

The current EU anti-money laundering framework (the 4th AMLD as amended by the 5th AMLD) now targets individuals that trade in works of art and considers them as obliged entities when they trade or act as intermediaries in the trade of works of art. This includes people involved in storing, trading or acting as intermediaries in the trade of works of art when carried out by free ports.

Ad hoc EU trade prohibitions: the EU has adopted ad hoc measures for the import of cultural goods into its customs territory from Syria and Iraq. Council Regulation (EC) No 1210/2003 of 7 July 2003 concerning 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 applying these regulations may sometimes be challenging because of the nature of the products (e.g. an object that is not illicit as such, but whose real provenance is difficult to establish). Interestingly, in the Member States that have managed to seize cultural goods originating from Iraq or Syria, this action is part of the daily work of the very same institutions that control the general import of cultural goods and implementing the relevant rules does not impose any additional burden on them.

In any case, while there are some EU rules, they are limited to specific regions and do not cover all cases of imports of cultural goods. This results in checks that are insufficient for addressing the risks.

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

Money laundering

The assessment of the money laundering vulnerability posed by the trafficking of looted artefacts and antiques shows that:

a) risk exposure

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

b) risk awareness

The sector seems more aware about the money laundering risk than the terrorist financing ones. In several Member States, high value dealers receive relevant training and guidance. However, there is a very low level of suspicious transaction reporting which raises questions on the understanding of the list.

c) legal framework and controls

Individuals trading in goods are subject to EU anti-money laundering requirements when they receive payments in cash of €10,000 or more. The current EU anti-money laundering framework also now considers people trading in works of art as obliged entities. In addition, in many Member States, regulations aiming at limiting cash payments have been put in place. However, as with terrorist financing, the current checks are insufficient to address the risks that looted goods may present.

In addition, the G7 members consider that artefacts trafficking represents a high risk and that further work must be done in this area.

Conclusions: Despite the fact that the risk awareness is higher than that for terrorist financing, the assessment's other elements have common features. These include a low level of reporting and no evidence that cash payment limitations have limited the risks. The level of money laundering vulnerability posed by the purchase of artefacts and antiques is therefore considered as <u>significant/very significant</u> (level 3/4).

Mitigating measures

<u>1) For the Commission</u>:

- On 13 July 2017 the European Commission tabled a proposal for a regulation on the import of cultural goods[84] to set out conditions and procedures for the entry of cultural goods into the EU's customs territory. The Commission is also carrying out a study on 'Improving knowledge about illicit trade in cultural goods in the EU, and the new technologies available to combat it'.[85]
- The Commission also adopted a proposal[86] to swiftly reinforce the EU framework on preventing the financing of terrorism by increasing the transparency of cash payments. This will be done by introducing a restriction on cash payments or by any other appropriate means. By restricting the possibilities to use cash, the proposal would help disrupt the financing of terrorism, as the need to use non anonymous means of payment would either deter the activity or help it be detected and investigated more easily. Any such proposal would also aim to harmonise restrictions across the EU to create a level playing field for businesses and remove distortions of competition in the internal market. It would also help with the fight against money laundering, tax fraud and organised crime.
- Member States should notify the measures taken by dealers in goods to comply with their AML/CFT obligations. This would enable the Commission to further assess the risks posed by service providers accepting cash payments. The Commission will also assess the benefits of making additional sectors subject to AML/CFT rules.

[84] Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods; PE/82/2018/REV/1; OJ L 151, 7.6.2019, p. 1–14.
[85] The publication of this study was initially planned for 2018/2019.
[86] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005, OJ L 284, 12.11.2018, p. 6–2.

- The issue of the burden of the proof and private sales should be tackled.

2) For Member States:

- Member States should duly consider the risks posed by cash payments in their national risk assessments and define appropriate mitigating measures. Member States should consider making those sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of their national risk assessment.
- Member States should encourage more cooperation between law enforcement and archaeologists, who are their 'eyes and ears' in this field.
- Member States should provide training for law enforcement officers (customs and police) and ensure cooperation and the exchange of information between customs, border guards and other authorities.
- Promote 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-raising campaign and promotion of measures to the art market and museums, such as robust due diligence, computerised inventorying obligations and the EU's formal recognition of existing codes of ethics or conduct for museums and the art market.
- Consider becoming party to the UNIDROIT and NICOSIA Council of Europe conventions — or adopting some of the measures set out in those conventions.
- Oblige companies involved in art dealing and storing antiques (known as 'freeports') to declare all suspicious transactions, and subject the owners of companies dealing in and storing art and antiques who become involved in the trafficking of such goods to effective, proportionate and dissuasive penalties, including criminal penalties where necessary.

3) For obliged entities

- Promote the use of written contracts to get a very detailed invoice with a clear description of the goods (e.g. value, product description and high quality picture), which would also allow the real beneficiary of the transaction to be identified.
- Encourage ending the practice of private transactions in cash to anonymous buyers.
- Promote the idea of a robust traceability system for both online and physical trade consistent with the whole anti-money laundering philosophy.

5. 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 the related product/activity concerned

In the EU, the diamond market is mostly limited to one country — Belgium, with Belgian diamond dealers having the predominant share of the EU's diamond market. 1,700 companies are officially registered as diamond traders with the Federal Public Service of Economy. Belgium's total imports and exports amounted to $48 billion in 2015 alone. The world's largest mining companies have an office in Antwerp and sell a large proportion of their goods directly to Belgian companies. Belgium has four diamond bourses that are members of the World Federation of Diamond Bourses. According to the 2015 data published by Antwerp's diamond office[87] 84% of all rough diamonds and 50% of all polished diamonds on the planet come from Antwerp.

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 buy gold and jewellery which is then sold in another country using false invoices and certificates, or are used directly to buy gold in the national territory and sold to a precious metals

[87] Antwerp World Diamond Centre, https://www.awdc.be/.

broker who then sells 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 such as gold and stones such as diamonds as they are inexpensive to store and easy to turn into cash.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to the purchase of gold and diamonds shows that terrorists exploit this method as it is easily accessible and 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 terrorist financing threat related to the purchase of gold and diamonds is considered as moderately significant/ significant (level 2-3).

Money laundering

The assessment of the money laundering threat related to the purchase of gold and diamonds shows that perpetrators have developed large money laundering schemes using this method. According to the FATF's analysis, this is a high-risk scenario, as gold and diamonds are easy to move across borders (hidden in a car for instance). International trade in gold has also been seen as a technique to launder criminal proceeds. The case in question involved the declared importation of gold from the UAE to an EU Member State, the resale of the gold to a second EU Member State and exportation from there back to the UAE. The carousel nature of the activity and the low quality fake gold transported in this case gives grounds to believe that the commodity trading was only conducted to justify criminal money transfers. This method is closely connected to the assessment of couriers with gold/diamonds (see specific section).

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

Vulnerability

Terrorist financing

The level of terrorist financing vulnerabilities related to the purchase of gold and diamonds shows that:

a) risk exposure

Some private sector representatives mention that the use of cash in the diamond trade has decreased thanks to the limits imposed by some national anti-money laundering laws (in some countries, payments in cash are limited to 10% of the total amount of the transaction, with a maximum of €3,000). However, there is no specific information available on the trade in gold where cash payments are still recurrently used with no possibility of identifying the parties involved in the transactions.

b) risk awareness

It is very low as far as terrorist financing risks are concerned. There is no specific framework in place to limit the transport and purchase of gold and diamonds. Due to the cross-border nature of such movements, it is difficult or even impossible to carry out checks.

For trade in diamonds, some national organisations of diamond dealers have developed an organisational framework for providing guidance, training courses and assistance with suspicious transaction reports, as well as help with risk analysis. These organisations may also provide 'know your customers' databases which include sanctions lists, information about politically exposed persons and/or lists of high-risk third countries. Some diamond traders ensure that identification and verification processes are carried out before a transaction involving payment via bank transfer.

Nevertheless, these practices are rather limited and not sufficiently widespread to consider that the sector is well aware of the risks.

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

c) legal framework and controls

Individuals trading in goods are subject to EU anti-money laundering requirements when they receive payments in cash of €10,000 or more. These anti-money laundering requirements are limited to payments in cash and do not take the risks posed by transactions using other means of payment into consideration.

For trade in diamonds, one of the largest groups of diamonds in Europe is subject to AML/CFT rules. Therefore, most EU diamond dealers are subject to registration requirements (following fit and proper checks — in particular from a beneficial owner point of view) and to inspections from their responsible authorities that are competent to check both compliance with anti-money laundering obligations and cash payments.

The EU has 'Kimberley' authorities[88] in six countries that check imported and exported shipments of rough diamonds, especially for the presence of a Kimberley certificate (Belgium, the UK, Germany, Czechia, Romania and Portugal). This means rough diamonds cannot be imported to or exported from the EU without a Kimberley certificate and without passing through one of the six dedicated Kimberly Process (KP) authorities. These six KP authorities are appointed by the European Commission and operate under their supervision. Therefore, the transport of rough diamonds is always subject to checks when entering or exiting the EU. Since trading in rough diamonds without a KP certificate is tantamount to 'illegal trade', the KP is a strong preventative measure against money laundering.

[88] The Kimberley Process (KP) is a commitment to remove conflict diamonds from the global supply chain. Today, participants actively prevent 99.8% of the worldwide trade. Since the KP was put in place in 2003, the identifiable trade in conflict diamonds has declined from 15% to less than 1%. https://www.kimberleyprocess.com/en/european-union-0.

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 EU country.

However, national laws are not currently harmonised either for diamonds or gold and this creates a risk of there being discrepancies in the obligations imposed (such as the registration) and the checks applied.

For gold, the lack of harmonised framework is also problematic for checks and enforcement.

The number of suspicious transaction reports is rather low for this category of obliged entities. Transactions are often face-to-face, which poses a specific challenge for protecting employees.

Conclusions: From the elements above, the level of terrorist financing vulnerability related to the purchase of gold and diamonds is considered as significant (level 3).

Money laundering

The level of money laundering vulnerability related to the purchase of gold and diamonds shows that

a) risk exposure

Some private sector representatives mention that the use of cash in the diamond trade has decreased thanks to limits imposed by some national anti-money laundering laws (in some cases, payments in cash are limited to 10% of the total amount of the transaction, with a maximum of €3,000). However, there is no specific information available on the trade in gold where cash payments are still recurrently used with no possibility of identifying the parties involved in the transactions.

b) risk awareness

It is very low as far as money laundering risks are concerned. There is no specific framework in place to limit the transport and purchase of gold and diamonds. Due to the cross-border nature of such movements, checks are difficult or even impossible to implement.

For trade in diamonds, some national organisations of diamond dealers have developed an organisational framework for providing guidance, training courses and assistance with suspicious transaction reports, as well as help with risk analysis. These organisations may also provide 'know your customers' databases which include sanctions lists, information about PEPs and/or lists of high-risk third countries. Some diamond traders ensure that identification and verification processes are carried out before a transaction involving payment via bank transfer.

Nevertheless, these practices are rather limited and not sufficiently widespread to consider that the sector is well aware of the risks. The diamond and gold sectors are mostly made up of small companies (often one-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 customer due diligence procedures.

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

c) legal framework and controls

Individuals trading in goods are subject to EU anti-money laundering requirements when they receive payments in cash of €10,000 or more. These anti-money laundering requirements are limited to payments in cash and do not take the risks posed by transactions using other means of payment into consideration.

For trade in diamonds, one of the largest groups of diamonds in Europe is subject to AML/CFT rules. Therefore, some EU diamond dealers are subject to registration requirements (following fit and proper checks — in particular from a beneficial owner point of view) and to inspections from their responsible authorities that are competent to check both the compliance with anti-money laundering obligations and cash payments.

The EU has Kimberley authorities in six countries that check imported and exported shipments of rough diamonds, especially for the presence of a Kimberley certificate (Belgium, the UK, Germany, Czechia, Romania and Portugal). This means rough diamonds cannot be imported to or exported from the EU without a Kimberley certificate and without passing through one of the six dedicated KP authorities. These six KP authorities are appointed by the Commission and operate under their supervision. Therefore, the transport of rough diamonds is always subject to checks when entering or exiting the EU. Since trading in rough diamonds without a KP certificate is tantamount to 'illegal trade', the KP is a strong preventative 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 EU country.

However, national laws are not currently harmonised either for diamonds or gold and this creates a risk of there being discrepancies in the obligations imposed (such as the registration) and the checks applied.

For gold, the lack of harmonised framework is also problematic for checks and enforcement.

The number of suspicious transaction reports is rather low for this category of obliged entities. Transactions are often face-to-face, which poses a specific challenge for protecting employees.

Conclusions: Although regulations in place in some Member States have increased the level of risk awareness, the sector is still not organised well enough to allow the implementation of efficient monitoring and guidance. The level of money laundering vulnerability related to the purchase of gold and diamonds is therefore considered as significant (level 3).

Mitigating measures

1) For Member States:

- Member States should duly consider the risks posed by cash payments in their national risk assessments and define appropriate mitigating measures. Member States should consider making those sectors particularly exposed to money laundering and terrorist financing risks subject to the AML/CFT preventative regime based on the results of their national risk assessment.

- Member States should ensure that competent authorities conduct sufficient unannounced spot checks at diamond companies and gold traders' premises to identify possible loopholes in compliance with customer due diligence requirements and involve diamond experts to check the flow of goods.

2) For obliged entities:

- Training on customer due diligence, in particular for small businesses.
  This role can filled by a sector federation or a diamond bourse in the case of diamond traders. The training may be about basic AML/CFT requirements such as how to identify clients, how to perform a risk analysis, what are ultimate beneficial owners, what is a financial intelligence unit and how do you notify one, etc.
- Promoting the use of written contracts to get a very detailed invoice with a clear description of the goods (e.g. value, weight, quality).

3) For the Commission:

- Under the new Cash Control Regulation, the definition of cash has been extended to cover not only banknotes but also other instruments or highly liquid commodities, such as cheques, traveller's cheques, prepaid cards and gold.

- Additional studies could be carried out to deepen the analysis on those economic sectors/ situations that are more exposed to AML/CFT risks.

Further typology work could be carried out to identify economic sectors particularly vulnerable to money laundering and terrorist financing 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.

6. 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 terrorist financing threat related to the purchase of other kinds of high value goods (other than gold, diamonds, artefacts and antiques) has not been considered as relevant from a terrorist financing perspective. Therefore, the terrorist financing threat is not part of this assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering threat related to the purchase of other kinds of high value goods (other than gold, diamonds, artefacts and antiques) shows that criminal

organisations have recurrently used this method, which is easy to access and does not require specific expertise (it includes trafficking in jewellery, cars, boats and watches).

Criminal cash is often converted into goods that are in high demand in foreign markets. Cars and other vehicles are one of the most commonly bought and exported commodity. Key markets are North Africa and the Middle East. Machinery is exported to Iraq and Kuwait; luxury watches, gold and jewellery are exported to the Middle East and North Africa; and food is exported to Africa.

In some EU jurisdictions the lack of cash payment restrictions makes them more attractive for cash-based TBML. In other jurisdictions — even in countries with restrictions and reporting obligations — the levels of reporting are very low. Traders in high value goods are among those with the least reporting requirements. In some cases, criminal clients bring business worth millions to the trader, which is another disincentive for reporting.

Chinese organised crime groups have been found to exploit luxury items (haute couture) and popular European high-status brands on the Chinese market. Illegal cash is supplied to Chinese nationals who use it to buy luxury goods. These luxury goods are predominantly sold online in China and the proceeds are used to make settlements in China. Chinese organised crime groups' illegal activities in Europe are the main source of criminal proceeds used to buy these items. These illegal activities include tax and duty fraud of Chinese cargo, counterfeiting of goods, drug trafficking, labour and sexual exploitation.

According to the law enforcement authorities' findings, until 2015–2016 Chinese nationals residing in the EU were used as money mules. They opened bank accounts, made cash deposits and transferred the money to China. Another method was to use the incoming Chinese tourists to transfer cash upon their return to China. Over time and thanks to interventions by law enforcement agencies, Chinese criminal groups switched to other techniques such as using shoppers to purchase luxury goods. After being purchased in Europe, these goods are taken to China where they are sold for a profit and the generated proceeds are transferred internally in China between the buyers of the goods and the criminal structures. This method is a way for the criminals to conduct the full money laundering cycle, to the point where they can freely use the proceeds in China to pay for new consignments of Chinese cargo, for example. When imported to Europe, these consignments will be undervalued and sold without documents. The generated cash will once again be laundered and taken from Europe to China, creating a criminal cycle that circumvents both law enforcement and tax authorities' interventions.

Conclusions: The level of money laundering threat related to the purchase of other kinds of high value goods is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to the purchase of other kinds of high value goods (other than gold, diamonds, artefacts and antiques) has not

been considered as relevant from a terrorist financing perspective. The terrorist financing vulnerability is therefore not part of this assessment.

Conclusions: Not relevant.

Money laundering

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

a) risk exposure:

It is difficult to pinpoint the different kinds of goods that may be used to launder money. However, trade on high value goods other than gold 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 money laundering 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 suspicious transaction reporting demonstrates that the understanding of the risk is really low.

c) legal framework and controls:

Individuals trading in goods are subject to EU anti-money laundering requirements when they receive payments in cash for €10,000 or more. However, this definition is rather general and does not specify which categories of traded goods fall under the scope of the AMLD. In addition, these anti-money laundering requirements are limited to payments in cash and do not consider the risks of transactions using other means of payment. Nevertheless, some Member States have put in place cash payment restrictions.

However, there are no harmonised national laws in place to address the risks of high value goods trading. It seems that the level of record keeping is very low and that there is an absence of checks.

Conclusions: Although the regulations in place in some Member States have increased awareness of the risks, the sector is still not adequately organised to implement efficient monitoring and provide guidance. The level of money laundering vulnerability related to the purchase of other kinds of high value goods is therefore considered as significant (level 3).

Mitigating measures

1) For the Commission:

The Commission has looked at the potential impact of cash payment restrictions and has published a report on the subject.[89] The report concludes that the Commission should not consider any legislative initiative on this matter at this stage. Restrictions on cash payments are a sensitive issue for people in the EU, many of whom view the possibility to pay in cash as a fundamental freedom, which should not be disproportionally restricted.

- Member States should notify the measures that dealers in goods covered by the AMLD apply to comply with their AML/CFT obligations. On this basis, the Commission could further assess the risks posed by providers of services that accept cash payments. The Commission will also assess the benefits of subjecting additional sectors to AML/CFT rules.

2) For Member States:

Member States should duly consider the risks posed by cash payments in their national risk assessments and define appropriate mitigating measures. 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 national risk assessment.

[89] Report from the Commission to the European Parliament and the Council on restrictions on payments in cash — COM(2018) 483 final: https://ec.europa.eu/info/sites/info/files/economyfinance/com_2018_483_f1_report_from_commission_en_v4_p1_981536.pdf.

7. Couriers in precious metals and stones

Product
Gold and other precious metals

Sector
/

Description of the risk scenario

This involves the cross-border movement of gold and other precious metals as well as precious stones. Perpetrators who have made cash from their illegal activities seek to convert it into gold and other precious metals or stones so that they can either repatriate funds or move these goods to locations where they can be more easily placed in the legal economy.

Couriers may use air, sea or rail transport to cross an international border, via for example:
- 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; or

- sophisticated concealments of gold within goods sent by regular mail or post parcel services.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to gold and other precious metals reveals few indicators that terrorist groups use or have the intention to use this channel to finance terrorist activities.

Gold or diamond couriers are not the most attractive and secure option for terrorist groups — although these assets are frequently exploited in war zones 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 are not a preferred method for terrorist groups who tend to favour the use of cash. The level of terrorist financing threat is therefore considered as somewhat significant to significant (2).

Money laundering

The assessment of the money laundering threat related to gold and other precious metals couriers shows that organised crime groups have used this method to launder the proceeds of crime. Unlike terrorist organisations, organised crime groups consider it to be an attractive way to launder the proceeds of crime. It requires more planning than moving cash, but does not need 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 inexpensive. Perpetrators therefore have the required capacity and intention to use this method. Law enforcement agencies 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/diamonds.

Investigations conducted in the EU show that one of the most relevant cash-related techniques is transforming cash to gold or jewellery. Some EU countries like Italy and Belgium have active gold markets. Alongside the legal market, information indicates that the gold is stolen and melted. After criminal cash is exchanged for gold it is exported to the Middle East and North Africa where there is a high market demand.

Conclusions: The level of money laundering threat related to gold and other precious metals couriers is considered as significant (level 3).

Vulnerability

Terrorist financing

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

a) risk exposure

The assessment of the terrorist financing vulnerability shows that the risk exposure is intrinsically linked to the cash-based activity (anonymity, speediness). The risk exposure is therefore particularly significant for this method.

b) risk awareness

The sector shows a limited awareness of the risks and the checks in place are particularly weak.

c) legal framework and controls

Until the new Cash Control Regulation enters into force there are no checks on the correctness of the mandatory declaration of transportation of precious metals/stones at the EU's external borders. These assets are not easy to detect. Checks in the destination countries outside the EU do not help to lessen the risks (conversion of gold/diamond into cash in destination country without customer due diligence).

Conclusions: Gold and other precious metals couriers are not properly monitored because of the limited awareness of the sector. The checks are weak and the reliance on cash increases the vulnerability. There are no checks in place for the movement of precious metals/stones declarations at the EU's external borders. The level of terrorist financing vulnerability related to gold and other precious metals couriers is therefore considered as very significant (level 4).

Money laundering

The assessment of the money laundering 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). The risk exposure is therefore particularly significant for this method.

b) risk awareness

The sector shows limited awareness of the risks and the checks in place are particularly weak. Law enforcement agencies have also noticed that criminal organisations take advantage of the vagueness of the EU framework, in particular for disclosure of cash payments.

c) Legal framework and checks

There are no checks in place through the mandatory declaration of transportation of precious metals/stones at the EU's external borders (i.e. this is not covered by the Cash Control Regulation). Such assets are not easy to detect. Checks in the destination

countries outside the EU do not help to lessen the risks (conversion of gold/diamonds into cash in destination country without customer due diligence).

Conclusions: Gold and other precious metals couriers are not properly monitored because of the limited awareness of the sector. The checks in place are weak and the reliance on cash increases the vulnerability. There are no checks in place for declaring movement of precious metals/stones at the EU's external borders. The level of money laundering vulnerability related to gold and other precious metals couriers is therefore considered as very significant (level 4).

Mitigating measures

As recommended by the SNRA 2017 the Commission has adopted a new Cash Control Regulation to further mitigate the risks described.

8. Investment real estate

Product
Purchase and sales of real estate

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

Description of the risk scenario

Money laundering through real estate is a growing, worldwide problem, estimated to have reached $1.6 trillion a year. Although the exact scale of illegal activity in the sector is difficult to estimate, in 2017 individuals or companies with a high money laundering risk have been thought to own more than £4.2 billion of property in London alone[90]. In France, the Financial Intelligence Unit TRACFIN has identified the real estate sector as a

[90] Faulty towers: Understanding the impact of overseas corruption on the London property market, Transparency International UK, March 2017: https://www.transparency.org.uk/publications/faulty-towers-understanding-the-impact-of-overseas-corruption-on-the-london-property-market/#.W9LY-LpuaUk.

primary channel for money laundering in the country. Out of a total of 62,000 suspicious reports sent to TRACFIN in 2016, only 84 came from real estate agents, despite nearly one million transactions taking place that year[91].

Perpetrators may invest, as non-residents, in a country (through visa systems) and develop ML/TF networks.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to investment in real estate has been considered together with the real estate investment-related money laundering schemes to hide the illegal origin of the funds. The terrorist financing threat therefore does not need a separate assessment.

Conclusion: The terrorist financing threat related to investment in real estate is considered as very significant (level 4).

Money laundering

The assessment of the money laundering threat related to investment in real estate has highlighted the recurrent use of real estate sector by organised crime groups to launder the proceeds 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 law enforcement agencies that real estate is frequently used in money laundering schemes and because their services may be combined with those provided by other non-financial professionals, the level of terrorist financing threat related to real estate is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to investment in real estate has been considered together with real estate investment-related money laundering schemes to hide the illegal origin of the funds. The terrorist financing threat therefore does not need a separate assessment.

Conclusion: The assessment of the terrorist financing vulnerability related to investment in real estate is considered as very significant (level 4).

Money laundering

[91] Le Monde, 'Blanchiment d' Argent: les agents immobiliers font-ils preuve de complaisance?', 29 December 2017: http://www.lemonde.fr/societe/article/2017/12/29/blanchiment-d-argent-les-agents-immobiliers-en-premiereligne_5235527_3224.html

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

a) risk exposure

Although it is decreasing in practice, cash can still be used to finance real estate transactions in some Member States. This increases the risk of anonymous transactions. Real estate agents are usually involved in a business relationship with other professionals, making it difficult to monitor the business relationship effectively (sectors rely on each other to carry out checks)[92], and therefore increasing the risk exposure. Real estate activities may be based on financial flows coming from outside the EU and high-risk customers, such as politically exposed persons.

b) risk awareness

The level of awareness is uneven in the sector, and particularly depends on the size of the organisation/company concerned. Bigger structures may be more aware of the risk of being misused and consider that they have a role to play in monitoring their customers. Some of them 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 enhanced due diligence is required.

For small entities, apart from legal professionals that are part of an umbrella organisation, the level of awareness is drastically lower because: (i) they are not necessarily integrated in a centralised organisational framework that provides guidance and training; (ii) they deal with a lower volume of sales and therefore may have difficulties in understanding and applying a complex anti-money laundering framework (this is the case in particular for single entrepreneurs); and /or (iii) they tend to rely on other sectors to conduct the customer due diligence.

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 is not known at the beginning of the business relationship. The level of awareness of small entities depends on how much training is available.

In any case, the 'scattering' of the obliged entities involved does not simplify the implementation of checks and the understanding of the customer due diligence 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, etc.).

c) legal framework and checks in place

[92] Nevertheless, ultimate responsibility lies with the respective professional, i.e. the professionals are not allowed to rely on each other (see Recital 35 and Article 25 of the 4th AMLD). In contrast, having more people performing their customer due diligence obligations may increase the chance of detecting anti-money laundering activities.

Real estate agents are subject to EU anti-money laundering requirements. Following the modifications introduced by the 5th AMLD, information on real estate ownership by any natural or legal person will be made centrally available for public authorities. This does not require the creation of a central real estate register. Alternatively, electronic data retrieval systems can be used.

However, when several obliged entities are involved in real estate transactions it makes it difficult for competent authorities to identify the role played by a real estate agent and to identify red flags. The legal practices and procedures for these real estate transactions differ between countries. In some countries, the estate agent can 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.

Suspicious transaction reporting is uneven, and is only satisfactory when done by 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 suspicious transaction reports). As a consequence, investigative authorities may conduct their own analysis but not on the basis of the real estate information. Private sector representatives consider it a major challenge to identify the beneficial ownership as it is currently not mandatory to register such information. This is particularly the case when the seller and buyer transact in 'trust'.

Practices in the sector differ with efforts being made by representative professional associations to promote awareness and good practice examples for their members.[93]

Conclusions: The real estate sector is not organised well enough to sufficiently raise risk awareness. The involvement of different kinds of obliged entities in a real estate transactions/ business relationships tends to dissuade the sector from conducting its own customer due diligence. Suspicious transaction reporting is not satisfactory. The checks are difficult to carry out and there is not always a sound information trail. The level of money laundering vulnerability related to the real estate sector is therefore 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 the real estate sector produce an annual report on supervisory measures that have been put in place to ensure that the sector accurately applies its AML/CFT obligations. Self-regulatory bodies should report annually on the number of suspicious transaction reports filed to the financial intelligence units.

[93] As an example of good self-regulatory practices, the representative organisation in Belgium has developed an online tool to gather information and transmit it to national authorities. This tool is currently being rolled out in all other EU countries and national authorities may provide support to facilitate compliance.

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

2) for Member States:

- 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 (e.g. estate agent, legal professional, financial institution).

3) Multilevel governance and local government: improving knowledge-exchange and cooperation:

European cities are particularly faced with the negative societal impact of money laundering in real estate. This was highlighted during the public hearing of the 'Tax3 Committee' of the European Parliament on 5 February 2019. In 2018, the city of Amsterdam hosted a three-day conference entitled 'Flying Money', on the impact of illegal money flows, where 14 European cities shared their experiences. One conclusion was that it would be useful to see how different levels of governance involved in the fight against money laundering in real estate (local, national and European) can further cooperate, share expertise and experiences and produce solutions, for instance in the field of further improving information-exchange within the EU and implementing trainings/guidance for the sector (and obliged parties).

9. Services provided by accountants, auditors, advisors, and tax advisors

Product
Services provided by accountants, auditors, tax advisors

Sector
External accountants, auditors, tax advisors

General description of the sector and the related product/activity concerned

Accountants, auditors and advisors work in diverse capacities and sectors: in small and large accountancy firms, SMEs, big companies, governments, non-profit organisations, education, etc.

When looking specifically at anti-money laundering, the profession is bound by national AML/CFT legislation and the application of FATF recommendations. The profession's other checks and mitigation practices include:

- screening procedures of BOs as part of the KYC/CDD process;
- use of new technologies such as data analytics, data and process mining, artificial intelligence, real-time transaction screening, block chain and smart contracts, which can help to combat fraud and money laundering risks.

Their diverse professional activities can be grouped as follows:

- **Accountants** help organisations prepare their financial and non-financial data to measure performance, including the social impact of their economic activities. In doing so, they help organisations manage and control risks, and provide checks and balances on good governance, ethics and sustainability. They also report these measurements to the outside world so stakeholders can base their decisions on the organisation's performance. In some instance, they can provide additional services (see advisors below).
- **Auditors**[94] certify information by giving an independent expert opinion to improve an organisation's information or its context. In the case of a statutory audit, they provide a legally mandated check of the financial accounts of large and medium-sized companies and form an opinion on them. In some instance, they can provide additional services (see advisors below).
- **Advisors:** Many organisations rely on the accountancy profession's advice, for example on finance, tax, corporate social responsibility, human resources, data protection and cyber security.

Tax advisors carry out a range of activities. The main tax advice activities can 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. inheritance, 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.

Tax advisors' main activities differ from country to country, depending on whether the tax profession is organised in a similar way to accountancy or to law.

[94] For further information on EU auditing law: https://ec.europa.eu/info/eu-law-topic/eu-auditing-law_en
On Auditing of companies' financial statements: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_en

- In seven out of 22 countries (BE, ES, GR, IE, PT, RO and SK), tax advisors 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 advisors may represent clients before tribunals in an appeals procedure.
- In eight countries (FI, IT, LV, LU, NL, PL, CH and UK), tax advisors may represent their clients before the court in the case of fiscal matters but not in criminal tax matters (in Luxembourg, this refers to representation by accountants before the court of first instance).
- In six countries (AT, CZ, DE, HR, RU and UA), tax advisors may also represent their clients in criminal tax matters (although that does not take place in practice in CZ and HR).
- In eight countries (AT, DE, FI, LV, NL, PL, RU and UA), tax advisors may represent their clients before the Supreme Court in tax matters although in Austria and Finland this applies only to the Supreme Administrative Court. In France, tax advisors are lawyers.

Whether or not tax advisor is a separate profession in a country, few tax advisors practice exclusively in tax. As tax is often related to other areas, it is common that tax advisors 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 EU directives have an impact on the tax profession:
- the Professional Qualifications (PQ) Directive 2005/36/EC;
- the 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 advisors have consumer clients; and
- Directive 2000/31/EC applies to cross-border tax advisory services.

The amended Audit Directive (2014/56/EU) and the Audit Regulation (537/2014/EU) which became applicable on 17 June 2016 and introduces stricter requirements on the statutory audits of public-interest entities, such as listed companies, credit institutions, and insurance undertakings. This is to reduce risks of excessive familiarity between statutory auditors and their clients, encourage professional scepticism, and limit conflicts of interest. The Regulation sets out requirement for the provision of non-audit services. In addition, it imposes an obligation for the external auditors to report to supervisors a material breach of rules or material threat or doubt concerning the continuous functioning of the audited entity.

Description of the risk scenario

Perpetrators may use or require the services of accountants, auditors or tax advisors, albeit with a moderate level of involvement of the professionals themselves, with the aim to:

- misuse client accounts;

- purchase real estate;

- create trusts and companies/ manage trusts and companies;

- undertake certain litigation, set up and manage charities;

- arrange over or under-invoicing or false declarations for import/export goods;

- provide assurance; and/or

- provide assistance with tax compliance.

Experts in these fields may be involved in money laundering schemes by helping create '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 structures, often set up in multiple jurisdictions including offshore centres, is complicated and requires professional regulatory and tax services.

Threat

Terrorist financing

The assessment of the terrorist threat related to services provided by accountants, auditors, advisors, and tax advisors has been considered together with money laundering schemes related to services provided by these professionals to hide the illegal origin of the funds (see below). The terrorist financing threat therefore does not need a separate assessment.

Conclusion: The assessment of the terrorist financing threat related to services provided by advisors and tax advisors is considered as very significant (level 4). The assessment of the terrorist financing threat related to certain additional services provided by accountants and auditors is considered as significant (level 3).

Money laundering

The assessment of the money laundering threat related to services provided by accountants, auditors, advisors, and tax advisors has some features in common with legal advice from legal professionals.

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

Law enforcement agencies have evidence that organised crime groups frequently use tax advisors advice and involve this sector in their money laundering schemes. Tax advisors' services are considered useful for setting up money laundering schemes because they are needed for certain types of activities and/or because access to specialised tax expertise and skills may help with the laundering of the proceeds of crime. Access to tax advisors' legal services is quite easy and does not require specific competences or expertise. Criminal organisations rely on these professionals' skills to set up money laundering scheme, so that they do not have to develop these competences themselves. There is also evidence that some criminals seek to co-opt and knowingly involve tax advisors in their money laundering schemes.

Professionals can be involved in the laundering process to various degrees. They can be consulted for advice on how to circumvent specific legal frameworks and how to avoid triggering red flags put in place by banking institutions. Or they can take a more proactive approach by directly assisting or orchestrating the laundering process. Often, however, perpetrators seek to involve tax advisors because the services they offer are essential to a specific transaction and they add respectability to that transaction.

Experts in these areas are among the professionals most used by organised crime groups to launder criminal proceeds due to the types of services that they can provide to their clients. They can set up corporate structures, design accounting systems, provide book-keeping services, prepare documentation (financial statements or references, fraudulent income and expenses), act as insolvency practitioners, and provide general accounting advice. Through these services, some accountants can help organised crime groups obscure their identity and the origin of the money that they handle.

Most of these services are used for legitimate purposes. However, they can also support a large range of money laundering schemes. These include fraudulent trading, false invoices, preparation of false declarations of earning, fraudulent bankruptcy, tax evasion and other types of abuse of financial records.

Conclusions: Services provided by advisors and tax advisors, auditors and accountants are frequently used in money laundering schemes and are seen by organised crime groups as a way to compensate for their lack of expertise. The level of money laundering threat related to services provided by advisors and tax advisors is therefore considered as very significant (level 4). The level of money laundering threat related to certain services provided by accountants and auditors is considered as significant (level 3).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to services provided by accountants, auditors and tax advisors has been considered together with money laundering schemes related to services provided by these professionals to hide the illegal origin of the funds. The terrorist financing threat therefore does not need a separate assessment.

Conclusions: Similar to money laundering, the assessment of the terrorist financing vulnerability related to services provided by accountants, auditors, advisors, and tax advisors is considered as significant (level 3).

Money laundering

The assessment of the money laundering vulnerability related to services provided by accountants, auditors, advisors, and tax advisors shows that:

a) risk exposure

Tax advisors could quite often become involved in the management of complex transactions involving tax-related advice. These transactions may expose the sector to high-risk customers (such as politically exposed persons) or to complex legal entities or legal arrangements where the identification of the beneficial owner is particularly challenging. This sector is also highly able to manage tax matters related to these complex legal entities and legal arrangements as that is their core business.

b) risk awareness

Accountants, auditors and tax advisors are required to adhere to strict ethical or professional rules, and they consider this to be a sufficient protection against money laundering and terrorist financing occurring in or through their sector. However, this sector may also be infiltrated by organised crime groups and some sectoral supervisory bodies are still not adequately equipped to detect this kind of abuse (i.e. proper test requirements are lacking in some jurisdictions).

This sector benefits from a strong organisational framework at EU level. For instance, the European Federation for Accountants and Auditors for SMEs (EFAA), an umbrella organisation for national accountants and auditors' organisations, has 17 members throughout Europe representing over 320,000 accountants, auditors and tax advisors. The Confédération Fiscale Européenne encompasses 26 national organisations from 21 European States, representing more than 200,000 tax advisors. Accountancy Europe is another example. It unites 51 professional organisations from 36 countries that represent close to one million professional accountants, auditors, and advisors.

The role of these organisations is to ensure the exchange of information about national laws relevant to their sector and to coordinate compliance with EU legislation. They also ensure that the professionals are aware of changes in EU legislation that affect their anti-money laundering obligations, for example.

For auditors the Audit Regulation has also created the CEAOB: Committee of European Audit Oversight bodies. The CEAOB is a framework for co-operation between national audit oversight bodies at EU level. Its role is to strengthen EU-wide audit oversight.[95]

Strong organisation does not necessarily guarantee high quality cooperation with competent authorities in all fields.[96] Furthermore, some competent authorities and financial intelligence units consider that accountants, auditors and tax advisors are still not adequately aware of the risks posed by opaque structures and the methods for obscuring the beneficial ownership. However, a two way flow of information is needed to improve the situation and the sharing of typologies and information by law enforcement agencies would enable a better assessment of risks.

---

[95] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-reforms-and-their-progress/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/committee-european-auditing-oversight-bodies_en

[96] Art 12(2) of the Audit Regulation imposes an obligation for the external auditors to report to supervisors a material breach of rules or material threat or doubt concerning the continuous functioning of the audited entity.

c) legal framework and controls

Accountants, auditors,[97] advisors, and tax advisors have been subject to the EU anti-money laundering requirements since 2001. They must 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; and (v) creation, operation or management of trusts, companies, foundations, or similar structures.

Tax advisors, advisors, accountants, and auditors are quite a complex and diverse professional sector. Generally speaking, the sector is characterised by long-term business relationships that increase professionals' ability to detect unusual transactions or behaviour. Nevertheless, when specific advice is sought on irregular or one-time transactions, the professional may carry out their task without having a full understanding of their customer's financial situation. This has an impact on their level of suspicious transaction reporting, which is still quite low but better than lawyers. The sector sometimes justifies this low level of suspicious transaction reporting by the fact that, in this field, the professional in charge does not process or initiate a financial transaction on their 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 suspicious transaction reports.[98]

Given that opaque structures can be created in many jurisdictions, including in offshore centres, professionals can take advantage of tax and regulatory differences to sell their services.

Conclusions: Accountants, auditors, advisors, and tax advisors are well organised. However, there are weaknesses in the way they carry out checks and manage risks. The level of money laundering vulnerability related to services from accountants, auditors, advisors and tax advisors is therefore considered as <u>significant</u> (level 3).

Mitigating measures

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

Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 has clarified its scope when covering external auditors, accountants and tax advisors, extending it cover any other person that provides material aid, assistance or advice on tax matters as their principal business or professional activity.

[97] The supervision of auditors of public interest entities is not in the hands of professional/self-regulatory bodies.
[98] See previous note.

As regards beneficial ownership, corporate entities and trust are required to hold information on who their beneficial owner is. Also, beneficial owners are now required to provide corporate entities with the information they need. Corporate entities and trusts have to give this information to their accountants.

Effective, proportionate and dissuasive measures or sanctions are applied in cases of non-compliance with these rules.

Directive 2018/822/EU comes into effect as from 2020 when intermediaries are required to submit information on reportable cross-border tax arrangements[99] to their national authorities.

Within this framework the Commission should carry on conducting:

- 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; and
- 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.

2) for competent authorities:

- Member States should ensure that competent authorities/self-regulatory bodies (where responsible for supervision), supervising external auditors, external accountants and tax advisors provide information on the supervisory measures they have put in place to ensure that the sector accurately apply its AML/CFT obligations. When receiving suspicious transaction reports, supervisors must report annually on the number of reports filed to the financial intelligence units.
- On-site inspections commensurate to the population of external 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 external accountants and tax advisors.

[99] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

Encourage a better understanding among external auditors, external accountants and tax advisors on how to interpret and apply the legal privilege. Member States should issue guidance on implementing 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 the same client.

10. Legal services 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 a lawyer, notary or other independent legal professional) — as regards:

- misuse of client accounts;

- purchase of real state;

- creation of trusts and companies/ management of trusts and companies; or

- undertaking certain litigation.

They may be involved in money laundering schemes by helping create '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 terrorist financing threat related to legal services provided by legal professionals has been considered together with money laundering schemes related services provided by these professionals to hide the illegal origin of the funds. The terrorist financing threat therefore does not need a separate assessment.

Conclusion: The assessment of the terrorist financing threat related to services provided by legal professionals is therefore considered as very significant (level 4).

Money laundering

The assessment of the money laundering threat related to legal services provided by legal professionals has some features in common with legal services provided by accountants, auditors and tax advisors.

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

- Law enforcement agencies report that organised crime groups frequently use legal services provided by legal professionals and involve this sector in their money laundering schemes. Legal professionals' services are considered useful for setting up money laundering schemes as they are needed for certain types of activities and/or because access to specialised legal and notarial skills and services may help with the laundering of the proceeds of crime. Lawyers are particularly prone to being misused by criminals

because engaging a lawyer adds respectability and an appearance of legitimacy to an activity even when the service provided can help criminals launder money.

Legal professionals can support money laundering either by using the tools already at their disposal (e.g. client accounts) or by helping their clients create and manage accounts, trusts and companies to conceal and/or legitimise the source of their funds.

There are many ways in which client accounts can be used to launder money, the most common of which are:

- performing financial transactions on behalf of a client, including offshore banking;
- accepting large cash deposits in the client's account followed by cash withdrawals or the issuance of cheques;
- purchasing real estate, companies or land on behalf of a client; and
- in some cases, using the personal account of the legal professionals themselves to receive and transfer funds.

Lawyers can help create and manage shell and legitimate companies by providing contracts and creating corporate accounts. Offshore companies and trusts are particularly attractive to organised crime groups due to their strict banking and legal and administrative secrecy regulations and practices and the anonymity that they provide. In addition to the legal advice and paperwork that they provide, legal professionals can also take an active role in managing a company and its assets. They can for instance represent their client in the purchase and sale of a company and are responsible for disposing of the financial assets by ordering money transfers, buying other companies or investing in real estate. Similarly, lawyers can hold a position within the company (e.g. owner, director, and administrator), further distancing their client from the criminal assets.

In most EU countries, lawyers provide the complete documentation for the foundation and registration of companies, transfer of ownership titles, opening of accounts in banks, invoices and international trading documents. The nature of this documentation is challenging for investigations due to the technicality and secrecy that it entails.

Criminal organisations do not consider access to legal professionals to be particularly complex. For them, relying on legal professionals' skills means that they do not need to develop these competences themselves. To launder money, some organised crime groups have infiltrated law firms, posed as phony solicitors or stolen the identity of lawyers.

Conclusions: According to information provided by law enforcement agencies, legal professionals are frequently used in money laundering schemes. Using the services of legal professionals helps organised criminal organisations to avoid developing their own knowledge and expertise, and provides a 'stamp approval' for their activities. The level of money laundering threat related to legal professionals (lawyers, notaries and other independent legal professionals) is therefore considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to legal service provided by legal professionals has been considered together with money laundering schemes related to services from these professionals to hide the illegal origin of the funds. The terrorist financing threat therefore does not need a separate assessment.

Conclusion: The assessment of the terrorist financing threat related to services provided by legal professionals is therefore considered as significant (level 3).

Money laundering

The assessment of the money laundering vulnerability related to legal advice provided by legal professionals shows that:

a) risk exposure

The risk exposure results from the nature of some services/activities provided by legal professionals (which require anti-money laundering compliance).

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

b) risk awareness

The sector is not homogeneously organised (scope of legal professionals varies from one Member State to another — this shouldn't be a risk in itself) even though some EU organisations play an important role in providing information on how to apply anti-money laundering/combating the financing of terrorism (AML/CFT) requirements, in providing guidance and facilitating the exchange of information. In particular, they help define a list of red flags that people working in the sector can use, e.g. client's behaviour or identity, concealment techniques (use of intermediaries, avoidance of personal contact), size of funds (disproportionate amount of private funding), etc. The profession already seems to be aware of some risks such a customer giving instructions about transactions from a distance or with no legitimate reason or when there are numerous changes in legal advisor in a short time frame or the use of multiple legal advisors with no good reason.

In general, the level of suspicious transaction reporting is very low when dealing with legal professionals (although suspicious transaction reports from legal professionals cannot be compared to legal reports from financial institutions, for example).

However, in some countries, self-regulatory bodies are regulated by the State and are independent, acting efficiently as intermediaries between the financial authorities and the professionals involved. They organise, examine and evaluate the facts, making it easier for the financial authorities to distinguish between money laundering and normal cases.

c) legal framework and controls

Notaries, lawyers and other independent legal professionals have been subject to EU anti-money laundering requirements since 2001. They must 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 estate 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. Legal services are also often carried out face-to-face, which is a specific challenge for employee protection. There are also differences between the various professions involved, since notaries, being professionals, also participate in the public duty, and have, in some Member States, the status of public office holders.

In any case, the protection of the anonymity of the legal professional reporting the suspicion should be totally guaranteed. In some Member States there is a risk that the name of the notary at the origin of the declaration could appear on the suspicious transaction report, in particular if it is followed by court proceedings. To avoid this, rules should be developed to prevent any disclosure of the origin of the suspicious transaction report.

The legal professional privilege (professional secrecy) 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). 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. 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 should be clarified.

Conclusions: The sector's awareness of the risks still appears to be limited. Despite the legal framework in place, supervision of the sector does not always ensure a proper monitoring of the possible money laundering abuses. The level of money laundering vulnerability related to legal advice provided by legal professionals is therefore considered as <u>significant</u> (level 3).

Mitigating measures

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

- In the context of Directive (EU) 2015/849 as amended by Directive (EU) 2018/843:

  - 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.

  - To better disseminate the EU anti-money laundering legal framework and to help ensure the effective and consistent application of EU law, the Commission should support training activities for the legal profession (lawyers and notaries).

  - To organise stakeholder consultations/discussions to help inform the Commission of the transposition of money laundering and terrorist financing directives across the EU and to raise awareness of and exchange best practices on different aspects of legal professionals' anti-money laundering compliance.

- Directive 2018/822/EU comes into effect as from 2020 where intermediaries are required to submit information on reportable cross-border tax arrangements[100] to their national authorities.

2) for competent authorities:

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

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

3) for Member States:

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

[100] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

Self-regulatory bodies should make an effort to increase the number of thematic inspections and reporting. They should also organise training courses to develop a better understanding of the risks and AML/CFT compliance obligations.

1. General description of the gambling sector

General description of the sector and related product/activity concerned

Under the current EU AML framework (the 4th AMLD), gambling services are defined as services which involve 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 this risk assessment, the gambling sector has been split into land-based (offline) and online gambling, with the land-based sector divided further into sections on betting, bingo, casinos, gaming machines, lotteries and poker. A further division into different online gambling products was not considered necessary, as the relevant risks, threats and vulnerabilities appear to be primarily linked to the nature of online transactions rather than to specific forms of online gambling.

All providers of gambling services are obliged entities under the 4th AMLD. Member States have an obligation to regulate and supervise them for terrorism financing and money laundering purposes and give their competent authorities enhanced supervisory powers to monitor them and to ensure that the persons who effectively direct the business of such entities and the beneficial owners of such entities are fit and proper.

Providers of gambling services must apply customer due diligence measures upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked. While Member States are allowed to exempt certain gambling services from some or all of the requirements laid down in the 4th AMLD following an appropriate risk assessment, this is not the case for casinos. The use of an exemption by a Member State should be considered only in strictly limited and justified circumstances, and where the risks of money laundering or terrorist financing are low, and such exemptions should be notified to the Commission. The 4th AMLD had to be transposed into national law by 26 June 2017, therefore the effects of the changes introduced by the Directive concerning the gambling sector are difficult to assess at this early stage.

There is no sector-specific EU legislation on gambling. Member States are free to set the objectives of their policy and to set the level of protection required for consumers and to prevent criminality, including money laundering. However, the provisions of the EU Treaties 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 in order to protect the public, they are

required to demonstrate that the measures in question are suitable and necessary 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 of both. In response to the societal, technological and regulatory challenges and developments, a significant number of Member States have reviewed or are in the process of reviewing their gambling legislation. These reviews take into account new forms of gambling services, which have led to an increase in gambling services offered by operators authorised in an EU Member State 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 EUR16.5 billion in 2015, and expected to rise to around EUR25 billion by 2020. The revenue of the offline/land-based gambling market is equally expected to increase from around EUR77.5 billion in 2015 to around EUR82-84 billion in 2020.

Through non-legislative actions, as set out in 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 for consumers, especially in light of evidence of risks associated with gambling that include the development of addictive disorders and other negative personal and social consequences. In particular, in a Recommendation on 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 needed to appropriately meet public interest objectives. Member States should designate competent authorities and lay down clear guidance for operators, including on anti-money laundering. The Commission also supports cooperation between the national regulatory authorities within the framework of the Administrative Cooperation Arrangement concerning online gambling services (signed by most European Economic Area Member States in 2015).

Controlling the growing numbers of so-called unauthorised gambling offers and channelling these into the authorised, regulated gambling sector comprise some of the largest and most challenging tasks for regulators. Across the EU, it is estimated that millions of consumers are gambling on unauthorised online gambling sites. Therefore, awareness needs to be raised about the inherent risks of unregulated gambling websites, such as fraud, that are outside any form of control at EU level. The extent of such unauthorised, usually online, gambling varies considerably among Member States depending largely on how well the authorised market functions.

The control of the unauthorised market, and its associated risks, is outside the scope of this report, 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.

2. 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'). A Member State may have a fixed number of operators (including a single monopoly provider) or a non-restricted number of operators, as long as they meet certain criteria. Minimum and/or maximum numbers of retail outlets per licenced provider can also be laid down.

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 (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 terrorist financing threat related to betting activities has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering threat related to betting activities highlights the following:

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

The level of this threat may vary depending on the type of organisation that hosts the betting. In the case of national sport betting monopolies, the risk of infiltrating the ownership of the betting operator itself is close to inexistent. However, it is possible that individual retailers, which the betting operators rely on 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 that allows for the identity of the beneficial owner to remain concealed, 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. Sports agents and intermediaries corrupt or intimidate players and/or referees to guarantee their desired outcome in a match, while other agents place huge amounts of money in online and offline bets outside the EU. In such cases, match-fixing requires contacts (and 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.

- the purchasing of **winning tickets** to ensure winnings may represent another criminal group's intent to launder money.

Conclusion: **Law enforcement authorities have identified several methods or channels that may be used by organised crime groups when addressing betting activities. Beyond the horizontal threat which is the risk of infiltration and ownership, the other significant aspect is match-fixing. Organised crime groups require moderate levels of planning, knowledge and expertise to use these methods, given that they are perceived as a rather attractive, secure and financially viable option.**

In that context, the level of the threat posed by money laundering to betting activities is considered as significant (level 3).

Vulnerability

Terrorist financing

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

Conclusions: not relevant

The assessment of the money laundering vulnerability related to betting activities highlights the following:

a) risk exposure:

Betting activities are characterised by significant volumes of speedy and anonymous transactions, frequently cash based. While the use of cash has been decreasing due to alternative betting methods, it still represents more than 50% of turnover in some countries. Many bettors use cash essentially for confidentiality or reputational reasons.

According to industry experts, possible red flags include:

- 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 financial intelligence units the betting sector is not sufficiently aware of the risks as shown by the low number of suspicious transaction reports, as well as their poor quality.

- vulnerability to money laundering risks is significantly increased by the reliance on distribution networks (kiosks, retailers, points of sale) which have 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 be able to detect suspicious transactions (e.g. cumulative bets, division of high bets or unusual bets), depending on the type of relationship that operators and retailers have. The number of suspicious transaction reports 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, financial intelligence units and other competent authorities have the wrong perceptions and lack understanding about the risk factors inherent to betting. It seems that financial intelligence units have already expectations on the type of suspicions a gambling operator should report (financial intelligence units expect suspicious cases of match-fixing while the operator tends to report irregular amounts in the transaction). Betting operators are suffering from a lack of feedback from financial intelligence units about the suspicious transaction reports.
In addition, betting operators are developing customer due diligence requirements that could mitigate the risks of money laundering; some betting operators are imposing systematic identification of winners (over a certain amount), focusing on the beneficial owner for instance. They could also offer different methods for paying out winnings to

limit the use of cash and deploy "players cards"[101] to increase operator's knowledge of its customers.

c) legal framework and checks:

Betting activities are covered by the EU AML framework since the 4th AMLD. However, based on the Directive's minimum harmonisation principles, there could still be discrepancies from one Member State to another in terms of regulation, supervision of the sector and enforcement of AML/CFT rules.

Certain Member States have in place legislation covering the money laundering aspects of betting, and/or specific requirements in licensing agreements. In these cases, regulations in place tend to be strict when it comes to granting an authorisation (fit and proper AML check of key personnel) and to carrying out ongoing reporting obligations. These reporting obligations must be met whenever 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 their lifestyle. This implies that an effective internal reporting process is required and both management and staff need to have a good knowledge of AML. In this respect, some national legislation requires the betting sector to conduct a sectoral risk assessment showing that suitable checks and procedures are in place.

However, competent authorities are still concerned about how to enforce checks, in particular monitoring bets to detect money laundering risks in real time and to possibly suspend bets in case of suspicion. Given the nature of betting activities (including high-volume or sometimes last-minute betting), it appears that putting in place an accurate customer due diligence regime is a challenge that needs to be addressed. The reliance on retailers presents an additional level of uncertainty in terms of customer due diligence, considering that some points of sale are not exclusively dedicated to betting and are not able to operate such checks (for example, bars, restaurants, supermarkets, book-shops or gas stations).

Conclusion:

Betting activities do not represent a homogeneous business model. Regarding the assessment of vulnerability, while it is undeniable that nationally some betting operators are well aware about their money laundering/terrorist financing risks and their corresponding obligations, it is still uncertain whether they are able to put in place accurate and comprehensive checks due to the characteristics of betting activities (significant volumes of speedy and anonymous transactions, often using cash). Current legislation or rules as regards licence conditions could be improved to better ensure sufficient checks, although the vulnerability assessment shows that

[101] "Players cards" are devices used by gambling services providers to track the time and amount of bets played by the players. The gains and losses appear under the form of "points" that the players accumulate. The "points" can then be redeemed for cash or merchandise.

betting operators are more aware of risks as they have started developing some mitigating measures (such as systematic checks above a threshold or alternative payment tools to limit the use of cash).

The apparent lack of understanding by competent authorities and financial intelligence units on the functioning of the betting activities is another obstacle to good AML/CFT risk assessment and guidance. The mitigation of AML/CFT risks is also weakened by the low level of feedback from financial intelligence units.

In that context, the level of money laundering 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 (financial intelligence units, law enforcement agencies, police, sectorial regulatory bodies such as gambling regulators) so they can better understand the risk factors inherent to betting activities and provide efficient guidance.
- Member States should ensure regular cooperation between relevant authorities and betting operators, which should focus on:
    - strengthening the detection of suspicious transactions and increasing the number and the quality of the suspicious transaction reports;
    - organising training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments of betting operators' products/business model;
    - ensuring supervisory authorities provide clearer guidance on AML/CFT risks, on customer due diligence and on requirements for reporting suspicious transactions and on how to identify the most relevant indicators to detect money laundering risks;
    - ensuring that financial intelligence units provide feedback to betting operators about the quality of the suspicious transaction report and ways to improve reporting, and about how information provided in the report is used, preferably within a set period of time;
    - developing standardised template(s) at EU level for suspicious transaction or suspicious activity reports taking into account specific characteristics of the gambling sector.

2) For the sector:

- Member States should ensure that betting operators organise regular training sessions for staff, compliance officers and retailers, focusing particularly on risks of infiltration or ownership by organised crime groups and regularly review risk assessments of their products/business model.

- Europol signed a Memorandum of Understanding with the Global Lottery Monitoring System (GLMS) to share information and to regularly consult over sport competition manipulations and related organised crime investigations.
- Europol and EU Member States work closely with the UEFA's betting fraud detection system that monitors more than 30,000 UEFA and European domestic matches each year.
- Member States should ensure that betting operators promote i) players' cards[102] or the use of electronic identification schemes in order to facilitate customer identification and to limit the use of cash, and ii) the use of 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, if not done already.
- Member States should ensure that betting operators promote systematic risk-based customer due diligence of the winners, and promote a lower threshold of winnings subject to customer due diligence (currently at €2,000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission:

The Commission could provide guidance on Article 11(d) concerning the implementation of customer due diligence in case of 'several operations which appear to be linked'.

[102] "Players cards" are devices used by gambling services providers to track the time and amount of bets played by the players. The gains and losses appear under the form of "points" that the players accumulate. The "points" can then be redeemed for cash or merchandise.

3. 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, that can be electronic, bearing numbers. Bingo is played by marking or covering numbers identical to numbers drawn by chance, whether manually or electronically. It is won by the player who first marks or covers the 'line' which is achieved when all five numbers on one horizontal row on one scorecard are drawn, or when the player is first to complete the 'house' or 'bingo' when 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 of 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 terrorist financing threat related to bingo has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering threat related to bingo shows that:

- as is the case for all other gambling activities, one of the threats posed by money laundering 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 type of operator organising the bingo activities. In bingo, it appears that infiltration occurs when street criminals run bars where bingo draws are not monitored and may be used for money laundering purposes (making the funds licit despite coming from an illegitimate origin).

- except the risk of infiltration, this risk scenario is rarely used by criminals to launder proceeds of crime as 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 of infiltration and ownership, bingo is not considered by law enforcement agencies and other competent authorities as an attractive option for laundering 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 winnings.

In that context, the level of the threat posed by money laundering to bingo is considered to be of low significance (level 1).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to bingo has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering vulnerability related to bingo highlights:

a) risk exposure

The scale of bingo's activities is rather limited and represents a low number of financial transactions. When played offline, the activity is mostly based on cash. It relies on relatively low stakes and winnings, with prices often being merchandise instead of cash money. It involves a 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 money laundering cases is due to the high level of awareness of money

laundering risks or rather to the low level of intent of criminal organisations to use this scenario.

c) legal framework and checks

Bingo activities are covered by the EU AML framework since the 4th AMLD. However, based on the Directive's minimum harmonisation principles, there could still be discrepancies from one Member State to another in terms of regulation, supervision of the sector and enforcement of AML/CFT rules.

Bingo does not exist in all Member States, but where it does, it should be subject to AML regulation. At national level, bingo operators may either be covered under the regulation dealing with casinos or they may benefit from a specific regulation (e.g. a 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 efficient checks are in place. Once again, the relatively low levels of amounts at stake and/or winnings are a factor in the overall vulnerability assessment.

Conclusion: The characteristics of bingo makes it to a low degree vulnerable to money laundering 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 efficient checks in place. The risk awareness component was not possible to assess properly due to the lack of reported cases. In that context, the level of vulnerability related to money laundering is considered to be of low significance (level 1).

Mitigating measures

Member States should ensure that bingo operators organise regular training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups and risk assessments of their products/business model, which should be reviewed regularly. In view of this Member States should also continue monitoring bingo activities to identify possibly future risks.

4. Casinos

Product
Casino (land-based/offline)

Sector
Gambling sector

General description of the sector and related product/activity concerned

In several countries (Belgium, Czechia, 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), the casino does not necessarily provide 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 have been covered by EU AML legislation for more than 10 years, and while Member States are allowed to exempt certain gambling services from some or all of the requirements laid down in the 4th AMLD following an appropriate risk assessment, this is not the case for casinos.

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 in a wide variety of games (with clearly defined rules). Casino staff (croupiers) interact with players in many well regulated games such as Baccarat roulette and Blackjack. If winning, the player receive chips at the table, which then have to be converted back to cash at a dedicated point of sale (thus legitimising illicit funds).

A perpetrator could use ‘mules’ or collaborators that buy chips on their behalf for illicit cash. The perpetrator will receive the chips in the casino and exchange them for cash, pretending that they won these chips in the games offered at the casino.

A perpetrator could also take advantage of the fact that certain casino games provide for a high return on stakes (depending on whether bets are high risk or low risk). 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 transfer funds from one casino to another (if legally allowed), giving another player access to chips. In such cases, casinos are used like financial institutions with funds being transferred from one account to another.

Threat

Terrorist financing

The assessment of the terrorist financing (terrorist financing) threat related to casinos has not been considered as particularly relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the threat posed by money laundering to casinos highlights, as is the case for all other gambling activities, **the risk of infiltration or ownership by organised crime groups**. Law enforcement agencies have indicated that casinos in particular would be exposed to infiltration threats. However, casinos which are run by 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. Also, stakeholders have pointed out that national licensing systems guarantee that the ownership (and any changes in ownership) takes place according to national laws and regulations. Under these laws national regulatory authorities carry out strong fit and proper checks as well as checks concerning the origin of the funds involved. They also vet operators, key staff and high-ranking employees. Stakeholders also point out that casinos typically have stringent systems in place to prevent fraud and safeguard against all criminal activity. Still, law enforcement agencies overall consider casinos to be the most exploited channel to launder money through gambling activities, although casino activities have been covered by earlier EU AML legislation.

Conclusions:

Casinos are considered to be exposed to infiltration threats, although for casinos owned by the State or public companies, this level of risk is lower. Nevertheless, law enforcement agencies still consider casinos the most exploited channel to launder money through gambling activities. Hence, the risk of casinos being exploited to money laundering appears high, and the level of the threat posed by money laundering to casinos is considered as very <u>significant</u> (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to casinos has not been considered as relevant. In this context, the terrorist financing vulnerability is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of money laundering vulnerability shows that the market varies 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 individuals or those 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 earlier on in the EU AML legislation has helped the sector to become more aware of risks. The legal framework already in place for casinos has, for example, created incentives to train staff and to improve checks. Casino staff is regularly informed of, and trained to identify, patterns and behaviours considered to represent money laundering threats. These training sessions include, for instance, measures and instructions on handling of cash. Many land-based casinos have developed inspections and check systems by external and independent testing institutes which reduce the vulnerability to money laundering and criminal activities. Furthermore, the vast majority of land-based casinos have a CCTV system in place that oversees the areas where transactions are being carried out. Some customer due diligence procedures are automatically carried out 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 has been reached, which is in most cases EUR 2,000, as provided for by the 4th 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). Enhanced customer due diligence 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 financial intelligence units, some weaknesses still remain as regards the scope of the customer due diligence measures (which do not seem to be well understood by the sector) and their implementation which is not considered as satisfactory by the supervisors in all cases: e.g. when checks on ID cards are carried out, but the record-keeping requirements are not fulfilled or of bad quality; due diligence carried out on a customer when he enters the casino but not when he purchases chips. However, although the level of suspicious transaction reports is uneven depending on the Member State concerned, the low number of these reports is justified as the sector is deemed to be 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 suspicious transaction reports, stakeholders have highlighted the lack of feedback from financial intelligence units. They also stress that the quality of the reporting would improve if financial intelligence units provided guidance and feedback, preferably within a set period of time. The lack of feedback from financial intelligence units on the reports submitted causes difficulties for casinos in individual cases (where it is unclear whether funds should be paid out to a player who may in turn take action against the casinos) and prevents improvements to AML practices in general.

c) legal framework and checks

The inclusion of casinos in the list of obliged entities in the 4th AMLD, as well as in earlier EU AML legislation, has undoubtedly played a role in the quality of the checks in place. It appears that, overall, casinos manage to address the need to put in place several layers of checks, knowing that most of the time several gaming activities may be played in a casino.

From competent authorities' point of view, fit and proper checks are mitigating the main vulnerability for casinos, i.e. infiltration. 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, law enforcement agencies are still identifying some weaknesses, which suggests that the current legal framework is not correctly applied. The number of money laundering cases investigated by law enforcement agencies seems to show that there is still room for improvement.

Conclusions:

Although the risk exposure remains quite high (significant number of financial transactions; cash based), the inclusion of casinos in the AML framework for more than 10 years has raised the level of awareness of the sector's vulnerability to money laundering. Checks are more efficient and the staff are better trained. However, some weaknesses remain as regards implementing AML/CFT requirements, particularly customer due diligence requirements. The extent of the reporting remains rather uneven from one Member State to another which may be due to the good level of supervision. In that context, the level of money laundering 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 (financial intelligence units, law enforcement agencies, police, sectoral regulatory bodies such as gambling regulators) so they can better understand the risk factors inherent to casinos and provide efficient guidance.

- Member States should ensure regular cooperation between relevant authorities and casinos, which should focus on:

- strengthening the detection of suspicious transactions and increasing the number and the quality of the suspicious transaction reports;
- organising training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments of betting operators products/business models;
- ensuring supervisory authorities provide clearer guidance on AML/CFT risks, on customer due diligence and on requirements for reporting suspicious transactions and on how to identify the most relevant indicators to detect money laundering risks.
- ensuring that financial intelligence units provide feedback to casinos about the quality of the suspicious transaction report, and ways to improve reporting, and about how information provided in the report is used, preferably within a set period of time;
- developing standardised template(s) at EU level for suspicious transaction or suspicious activity reports, taking into account specific characteristics of the gambling sector;
- recommending the non-issuing of winning ticket certificates in casinos.

- Member States should require competent authorities to provide a report on whether casinos apply the AML/CFT regime effectively, concerning in particular the effectiveness of the checks undertaken through CCTV and the effectiveness of the threshold-based customer due diligence.

2) For the sector:

- Member States should ensure that casinos organise regular training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly review risk assessments of their products/business model.
- Member States should ensure that casinos promote i) players' cards[103] or use electronic identification schemes in order to facilitate customer identification and to limit the use of cash and ii) the use of real-time monitoring systems to identify suspicious transactions.
- Member States should ensure that casinos designate an AML officer at the premises, if not done already.
- Member States should ensure that casino operators promote systematic risk-based customer due diligence of the winners, and promote a lower threshold of winnings subject to customer due diligence (currently at €2,000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission:

[103] "Players cards" are devices used by gambling services providers to track the time and amount of bets played by the players. The gains and losses appear under the form of "points" that the players accumulate. The "points" can then be redeemed for cash or merchandise.

The Commission could provide guidance on Article 11(d) concerning the implementation of customer due diligence in the case of 'several operations which appear to be linked'.

5. 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, depending on the maximum stake, maximum winnings or the type of premises the gaming machine can be placed in. A further distinction is made between traditional slot machines ('fruit machines') and video lottery terminals which are connected to a central terminal and offer a wider range of games.

The market for gaming machines outside casinos in the EU varies from one Member State to another (or region as authorisations may be granted and supervision assured at this level). In certain Member States, gaming machines are prohibited outside casinos, while 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, presenting 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. However, 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 the perpetrator can request the pay-out of the remaining funds into a bank account or in cash with a receipt (thereby providing opportunities for legitimising a larger sum than actually gambled).

A perpetrator uses electronic roulette to launder money by 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[104] 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 minimise suspicion or bypass limits on stakes or playtime.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to gaming machines has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the threat posed by money laundering to gaming machines highlights, as for all other gambling activities, **the risk of infiltration or ownership by organised crime groups**. However, according to investigations by law enforcement agencies, it seems that cases are quite rare or are 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 recover immediately the funds.

Conclusions: Gaming machines do not appear as an attractive option for money laundering due to the inherent chance element, low amounts of stakes and winnings combined with the time and effort required to launder any significant amounts of money. However, certain types of gaming machines allow for deposits of higher stakes and/or provide higher winnings; or they allow the perpetrator 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 threat posed by money laundering may vary between different types of gaming machines (low/high stakes and/or winnings) it is generally considered as <u>moderately significant</u> (level 2).

Vulnerability

Terrorist financing

[104] "Ticket-in, ticket out (TITO)" machines are used in casino slot machines to print out a slip of paper with a barcode indicating the amount of money represented. These can in turn be redeemed for cash at an automated kiosk.

The assessment of the terrorist financing vulnerability related to gaming machines has not been considered as relevant. In this context, the terrorist financing vulnerability is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering vulnerability related to gaming machines highlights:

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 of their AML/CFT obligations, as they are less organised than when operators in land-based casinos.

Competent authorities have, in addition, noticed the emerging risk linked to video lottery terminals which trigger a growing number of suspicious transaction reports (because in general, the winnings are re-inserted into the dark economy).

c) legal framework and checks in place

Gaming machines are covered by the EU AML framework since the 4th AMLD). However, based on the Directive's minimum harmonisation principles, there could still be discrepancies from one Member State to another in terms of regulation, supervision 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 financial intelligence units, the level of checks is insufficient and the level of sanctions not dissuasive enough (e.g. a bookmaker in Member State X received a fine of more than €100,000 for failing to prevent a drug dealer from laundering over €1 million in its outlets). However, gaming machines operators are currently developing some mitigating measures, such as prohibiting pay-out of winnings in cash when they exceed certain amounts.

Conclusions:

For gaming machines outside casinos, it appears that the checks in place are not efficient and that the level of suspicious transaction reporting is quite low, although mitigating measures in order to limit the pay-out in cash tend to limit the risk of money laundering. Even if the amounts of stakes and winnings are often relatively low, gaming machines allow for speedy and anonymous (as well as repeated)

transactions, often cash based. Transactions can also be carried out in multiple venues to minimise suspicions or bypass limits on stakes or playtime. In that context, the level of vulnerability to money laundering for gaming machines is considered as moderately significant (level 2).

Mitigating measures

1) For competent authorities

- Member States should improve cooperation between relevant authorities (financial intelligence units, law enforcement agencies, police, sectoral regulatory bodies such as gambling regulators) so they can better understand the risk factors inherent to gaming machines and provide efficient guidance.
- Member States should ensure regular cooperation between relevant authorities and gaming machine operators, which should focus on:
    - strengthening the detection of suspicious transactions and increasing the number and the quality of the suspicious transaction reports;
    - organising training sessions for staff, compliance officers and retailers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments;
    - Ensuring supervisory authorities provide clearer guidance on AML/CFT risks, on customer due diligence and on requirements for reporting suspicious transactions and on how to identify the most relevant indicators to detect money laundering risks;
    - ensuring supervisory authorities provide clearer guidance on emerging risks linked to video lottery terminals;
    - ensuring that financial intelligence units provide feedback to gaming machine operators about the quality of the suspicious transaction report and ways to improve the reporting, and about how the information provided in the report is used, preferably within a set period of time;
    - developing standardised template(s) at EU level for suspicious transaction or suspicious activity reports, taking into account specific characteristics of the gambling sector.

2) For the sector

- Member States should ensure that operators of gaming machines organise regular training sessions for staff, compliance officers and retailers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly review risk assessments of their products/business model.
- Member States should ensure that operators of gaming machines promote i) players' cards[105] or the use of electronic identification schemes in order to facilitate customer identification and to limit the use of cash, and ii) real-time monitoring systems to identify suspicious transactions at point of sale.;

[105] "Players cards" are devices used by gambling services providers to track the time and amount of bets played by the players. The gains and losses appear under the form of "points" that the players accumulate. The "points" can then be redeemed for cash or merchandise.

- Member States should ensure that gaming machines operators designate an AML officer at the premises, if not done already.
  Member States should ensure that betting operators promote systematic risk-based customer due diligence of the winners, and promoting a lower threshold of winnings subject to customer due diligence (currently at €2,000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission

The Commission could provide guidance on Article 11(d) concerning the implementation of customer due diligence in case of 'several operations which appear to be linked'.

6. Lotteries

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 which have been granted an exclusive licence to operate lottery games in a Member State's territory (state-owned and private operators, both profit and non-profit, who operate on behalf of the state), to small charity lotteries that generate revenues for both the public benefit or for non-profit organisations (e.g. charities, civil society, sport, culture, heritage, social welfare). The definition of a lottery — or the requirements to obtain a licence — varies from one Member State to another.

National lottery tickets are normally sold through agents for cash or through card transactions, or directly to the player online. Small amounts are played in most cases. Winners can be selected instantly (e.g. 'scratch- cards') or on the basis of weekly draws (often highly promoted and televised). Winnings are either paid out by the agents when the winning ticket is presented (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 winning a jackpot is very low (e.g. the probability is in the range of one in 140 million for Euro Millions rank 1 jackpot).

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. Purchasing lottery tickets directly to win a prize is therefore not considered a likely risk scenario. On the contrary, the method 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 a more viable scenario reported by law enforcement agencies.

Threat

Terrorist financing

The assessment of the terrorist financing (threat related to lotteries has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the threat posed by money laundering to lotteries shows that:

- as it is the case for all other gambling activities, **there is a risk of infiltration or ownership by organised crime groups.** In case of State-owned lotteries, the risk seems minimal, but increases at retailer-level.

- for other kinds of threats, according to law enforcement agencies, criminals have only vague intentions of using lotteries to launder proceeds of crime. Few cases have been identified by law enforcement agencies where, for example, winning tickets have been found together with cash or drugs in seizures. However, if and when used, this scenario may allow large sums of cash to be collected (e.g. €1.2m was collected via winning tickets in a recent investigation). However, some planning capabilities and technical expertise are needed which in general requires the complicity of the lottery operator and the reliance on frontmen. This could limit criminals' intent to use this risk scenario. Also, lotteries offer less opportunities in terms of money laundering due to lower frequency of draws, 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 for laundering proceeds of crime due to the relatively low return rate (most of the time only 50% of the ticket sales are used for prizes).

Conclusions: There have been reported cases of lotteries being used to launder proceeds of crimes. However, it requires planning and expertise that may limit the intent and capability of organised crime organisations to use it. The specific method of purchasing winning tickets appears though to be a more viable and reported scenario. In this context, the level of the threat posed by money laundering to lotteries is considered as moderately significant (level 2).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to lotteries has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering vulnerability related to lotteries highlights:

a) risk exposure

In assessing the level of risk exposure, it is also taken into consideration that in many Member States lotteries are run by a State monopoly. Payments of higher winnings are subject to rigorous checks 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), which vary between 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, in order for it to be purchased for criminal purposes, unless they are actively helped by accomplices.

b) risk awareness

While the misuse of lottery games via the purchase of winning tickets is considered as a major concern for financial intelligence units and law enforcement agencies (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 programmes in AML awareness/detection.

c) legal framework and checks

Lotteries are covered by the EU AML framework since the 4th AMLD. However, based on the Directive's minimum harmonisation principles, there could still be discrepancies from one Member State to another in terms of regulation, supervision of the sector and enforcement of AML/CFT rules.

However, at national level, supervision by competent authorities works well and is generally undertaken by public authorities. For example, it has been pointed out that most gambling authorities have already introduced recommended procedures and checks to deter criminals from using the lottery facilities for money laundering. Additionally, lottery operators have established internal checks and heightened vigilance in these matters. For example, most Member states already have a procedure in place to verify a jackpot winner's identity where the prize exceeds a predetermined threshold.

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 (the purchasing of) winning tickets. National frameworks in place have introduced measures to check the identities of winners, in particular those with high winnings. Still, the (purchasing of) winning tickets risk scenario remains a major point of concern. On this basis, the level of vulnerability to money laundering for lotteries is considered as moderately significant (level 2).

Mitigating measures

1) For competent authorities:

- Member States should improve cooperation between relevant authorities (financial intelligence units, law enforcement agencies, police, sectoral regulatory bodies such as gambling regulators) so they can better understand the risk factors inherent to lottery activities and to provide efficient guidance.
- Member States should ensure a regular cooperation between relevant authorities and lotteries operators, which should focus on:
    - strengthening the implementation of consumer due diligence requirements and the detection of suspicious transactions especially in the context of winning tickets, as well as increasing the number and the quality of suspicious transaction reports;
    - organising training sessions for staff, compliance officers and retailers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments of their products/business model;
    - ensuring supervisory authorities provide clearer guidance on AML/CFT risks, on customer due diligence and on requirements for reporting suspicious transactions and on how to identify the most relevant indicators to detect money laundering risks;
    - ensuring that financial intelligence units provide feedback to lottery operators about the quality of the suspicious transaction report and ways to improve the reporting, and about how the information provided in the report is used, preferably within a set period of time;
    - developing standardised template(s) at EU level for suspicious transaction and suspicious activity reports, taking into account specific characteristics of the gambling sector.

2) For the sector:

- Member States should ensure that lottery operators regularly organise training sessions for staff, compliance officers and retailers, which focus particularly on risks of infiltration or ownership by organised crime groups, and regularly review risk assessments of their products/business model. Training would also include items related to appropriate red flags on repetitive winnings.

- Member States should ensure that lotteries promote i) the use of systems for systematically identifying winners, such as players' cards[106] or electronic identification schemes, in order to facilitate customer identification, and ii) 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, if not done already.
- Member States should ensure that betting operators promote systematic risk-based customer due diligence of the winners, and promoting a lower threshold of winnings subject to customer due diligence (currently at €2,000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission:

The Commission could provide guidance on Article 11(d) concerning the implementation of customer due diligence in case of 'several operations which appear to be linked'.

7. 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, at least some of which remain hidden until the end of the hand, and the bets.

Poker is organised 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 organised as a tournament, where a poker player enters by paying a fixed buy-in at the start and is given a certain number 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 organiser of the activity. The organiser will receive a fixed amount of the turnover (a rake) or winnings.

[106] "Players cards" are devices used by gambling services providers to track the time and amount of bets played by the players. The gains and losses appear under the form of "points" that the players accumulate. The "points" can then be redeemed for cash or merchandise.

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 (folding 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 be invitation only.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to poker has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the threat posed by money laundering to poker shows that

- as for all other gambling activities, **there is a risk of infiltration or ownership by organised crime groups.**

- this channel is perceived as rather attractive although it requires moderate levels of planning (complicity) or technical expertise (gaming strategy itself) to make use of illicit tournaments or to deliberately lose so that an accomplice can win.

Conclusions: In addition to the risk that a company holding a licence to organise poker games or tournaments in physical premises could be infiltrated (which is a horizontal threat that is also valid for other gambling service providers) in some Member States it is possible to organise individual tournaments, which could result in criminal organisations legally organising poker games/tournaments. The peer-to-peer gambling nature of poker (the possibility for deliberate losses/ ensuring another player gets the winnings) makes poker attractive for money laundering, although it requires some expertise and planning. In that context, the level of the threat posed by money laundering to poker is considered as <u>significant</u> (level 3).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to poker has not been considered as relevant. In that context, the terrorist financing threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering vulnerability related to poker highlights

a) risk exposure

Most of the time, poker games are organised within 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 involves cash-based transactions and players playing against other players known as the 'peer-to-peer element' (involving deliberate losses or ensuring winnings go to another player). Poker games allow significant volumes of speedy and anonymous transactions to be carried out between players (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. Carrying out a dedicated analysis is challenging.

c) legal framework and checks

Poker activities (outside casinos) are covered by the EU AML framework since the 4th AMLD. However, based on the Directive's minimum harmonisation principles, there could still be discrepancies between Member State in terms of regulation, supervision of the sector and enforcement of AML/CFT rules.

Players play against other players and there are no records on 'who-lost-to-whom' Unauthorised private poker clubs have also emerged, which are well organised and compete with the legal sector. Financial intelligence units believe that these clubs have only a low capacity for detecting suspicious transactions, especially because the sector itself is not well aware of the risks and/or not sufficiently regulated/supervised at national level.

Conclusions:
Considering the 'peer-to-peer element', the apparent lack of record keeping and proper supervision and that the sector itself is not well aware of the risks and/or well-equipped to tackle money laundering abuses, the level of vulnerability to money laundering for poker is considered as significant (level 3).

Mitigating measures

1) For competent authorities:

- Member States should improve cooperation between relevant authorities (financial intelligence units, law enforcement agencies, police, sectorial

regulatory bodies such as gambling regulators) so they can better understand the risk factors inherent to poker and provide efficient guidance.

- Member States should ensure a regular cooperation between relevant authorities and poker operators, which should focus on:
    - strengthening customer due diligence requirements and the detection of suspicious transactions, and increasing the number and the quality of the suspicious transaction reports;
    - organising training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments of their products/business model;
    - Ensuring supervisory authorities provide clearer guidance on AML/CFT risks, on customer due diligence and on requirements for reporting suspicious transactions and on how to identify the most relevant indicators to detect money laundering risks;
    - ensuring that financial intelligence units provide feedback to poker operators about the quality of the suspicious transaction report, and ways to improve reporting, and about how information provided in the report is used, preferably within a set period of time;
    - developing standardised template(s) at EU level for suspicious transaction and suspicious activity reports taking into account specific characteristics of the gambling sector.

2) For the sector:

- Member States should ensure that poker operators organise regular training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly review risk assessments of their products/business model.
- Member States should ensure that poker operators promote player's cards, or use electronic identification schemes in order to facilitate customer identification;
- Member States should ensure that poker operators designate an AML officer at the premises, if not done already;
- Member States should ensure that betting operators promote systematic risk-based customer due diligence of the winners, and promoting a lower threshold of winnings subject to customer due diligence (currently at €2,000 as provided by Article 11 d) of Directive (EU) 2015/849).

3) For the Commission:

The Commission could provide guidance on Article 11(d) concerning the implementation of customer due diligence in case of 'several operations which appear to be linked'.

8. Online gambling

Product
Online gambling

Sector
Gambling sector

General description of the sector and related product/activity concerned

For this purpose of this report, online gambling means any 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 by any means at a distance, by electronic means or any other technology that facilitates communication, and at the individual request of a recipient of services.

All gambling products are available online. These include i) games where the customer wagers a stake against the gambling service provider at fixed odds (e.g. lotteries, sports betting, roulette, etc.) and ii) gambling activities where customers can play against each other and where the service provider takes a small commission for facilitating the activity, usually a percentage of net winnings for each customer on each event (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 report, as the relevant risks, threats and vulnerabilities

appear to be primarily linked to the nature of online transactions 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 due to use of the internet. At the same time, electronic gambling offers a significant mitigating feature — the possibility to track 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'[107] 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 if 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 terrorist financing threat related to online gambling has not been considered as relevant to this first supranational risk assessment report. Therefore, this threat is not part of the assessment.

Conclusions: not relevant

Money laundering

The assessment of the money laundering threat related to online gambling shows that:

- as for all other gambling activities, **there is a risk of infiltration or ownership by organised crime groups.** Law enforcement agencies have several examples of such cases.

[107] A *smurf* is an experienced player who uses a new account to play "anonymous" on a game server to deceive other players into thinking he's new to gambling. The goal is to create new accounts by starting from scratch, so as to confront players of lower level.

- in addition, organised crime groups may easily access to such a channel in which it is cheap and practical for them to set up their activities. Online gambling represents an attractive tool to launder proceeds of crime. It could allow criminal money to be easily converted into legitimate gambling earnings. It involves a huge volume of transactions and financial flows. Europol indicated that recent cases showed that some criminal networks used the legal online betting and gambling circuit of companies located in some Member States for money laundering.

Online gambling in virtual assets provides a great opportunity for cybercriminals and this technique was used in recent ransomware attacks. Among the known types of activities are the following:

- Online gambling accounts are credited with dirty funds (cashing in) followed by the gambling of a small amount of funds, transferring the remaining amount to a different player (or to a different gambling operator). The remaining funds are cashed out as legitimate gambling earnings.
- The use of 'smurfs' betting directly against each other using dirty funds. One of the 'smurfs' receives all the funds as an apparent winner, who will then cash them out as legitimate gambling earnings.
- The purchase of online casino accounts containing funds already uploaded by non-criminal players at a higher price than the real one.
- The operator is used as a cash intensive business to mix dirty money from criminal activities with clean money from legitimate customers.
- Criminals fix gambling odds and outcomes so that 'smurfs' can bet dirty money on the pre-selected losing outcomes, to the benefit of the online casino ('ghost matches').
- Criminals use third parties operating as 'smurfs', and create fictitious customer accounts to gamble and lose dirty money over the internet. All gambled funds are accounted for as profits of the online casino and due taxes are paid.

Additionally, different types of bets exist in the online environment that are not available offline. There is a specific risk for sure bets in online betting, where a player uses several accounts to place bets on every possible outcome and thereby reduces the risks of loss. In the case of online poker, there is also a specific risk for collusion.

- risks associated with the lack of face-to-face contact although the anonymity can be minimised by proper checks and verification measures, as well as traceability and tracking of electronic transactions depending on the level of supervision by relevant authorities.

Conclusions: Law enforcement agencies 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 the threat posed by money laundering to online gambling is considered as <u>significant</u> (level 3).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to online gambling has not been considered as relevant. In that context, the threat posed by terrorist financing is not part of the assessment.

Conclusions: not relevant.

Money laundering

The assessment of the money laundering vulnerability related to online gambling highlights

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 high risk both in the EU framework and in Financial Action Task Force 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 it more difficult to detect any suspicions. Although online gambling is not based on cash, it is closely connected to the use of other products such as e-money or virtual currencies, which present their own set of money laundering risks. However, the risk exposure of anonymous/pre-paid cards has now been tackled with the limitations introduced in the 4th AMLD and in the upcoming transposition of the 5th AMLD, that will substantially reduce the possibility to use such means of payments. Additionally, providers of exchange services between virtual currencies and fiat currencies as well as custodian wallet providers[108] will be considered as obliged entities under the 5th AMLD. The customer due diligence procedures they will have to apply should also bring more transparency in the context of online gambling. The non-face-to-face nature of online gambling increases the degree of anonymity, even though initiatives like eIDAS should also help in partially mitigating the risk associated with this dimension of the business by better enabling 'know your customer' procedures to be conducted. Also, law enforcement agencies (including EUROPOL) have noticed an increased trend in the creation of unlicensed gambling sites which are not subject to customer due diligence, record-keeping and reporting requirements. They are not audited by a supervisory authority. This may have major effects on the EU internal market when these unlicensed gambling sites are incorporated outside the EU and engage easily with EU customers over the internet.

[108] An entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies

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 customer due diligence.

b) risk awareness

The level of awareness in the online gambling sector should have increased since the inclusion of the sector in the EU AML framework When covered by the AML/CFT requirements, the level of suspicious transaction reporting is quite good and automatic checks are 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.

In large parts of the sector AML training session have been provided for every employee within a company. Employees are also trained on the practical issues such as the characteristics of the suspicions, how to bring them to the attention of the compliance officer and how to tackle the issues on an operational level. Representatives of online gambling operators note that financial intelligence units do not offer feedback on suspicious transaction reports that are 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 being made 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 time competent authorities provide risk assessment in order to help obliged entities improve 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 must 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 checks

The whole online gambling sector is covered by the EU AML framework since the 4th AMLD. However, based on the Directive's minimum harmonisation principles, there could still be discrepancies from one Member State to another in terms of regulation, supervision of the sector and enforcement of AML/CFT rules.

Some operators licensed in one or more Member States also offer gambling services 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 EU control).

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 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 should occur (host/home FIU) and where the supervisory actions should take place (host/home supervisors). Hence, competent authorities and obliged entities consider that the current legal framework is

not always clear enough on which authority is competent to apply AML/CFT requirements.

There is no duty of mutual-recognition of authorisations issued by the European Economic Area 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, regulations and checks in place vary.

Conclusions:

Despite several risk-based measures already being implemented by many online operators (for example anti-money laundering training sessions for employees, customer due diligence and 'know your customer' processes), the exposure to money laundering risks in online gambling is still rather high as it encompasses significant factors such as the non-face-to face element, huge and complex volumes of transactions and financial flows. Although not based on cash, it is closely connected to the use of e-money, and digital and virtual currencies which, for example, also increases the degree of anonymity for customers. As recognised, in many Member States, online gambling operators have developed a good level of self-regulation and risk assessment, although their cooperation with competent authorities and financial intelligence units could be improved. Operators believe that they do not get from clear guidance on how to properly address the risks considering, in particular, the lack of feedback from financial intelligence units on suspicious transaction reports. In that context, the level of money laundering vulnerability related to online gambling is considered as <u>significant</u> (level 3).

Mitigating measures

<u>1) For competent authorities/regulators:</u>

- Member States should improve cooperation <u>between relevant authorities</u> (financial intelligence units, law enforcement agencies, police, sectoral regulatory bodies such as gambling regulators) so they can better understand the risk factors inherent to online gambling and provide efficient guidance.
- Member States should ensure regular cooperation <u>between relevant authorities and online gambling operators</u>, which should focus on:
    - strengthening customer due diligence requirements and the detection of suspicious transactions, and increasing the number and the quality of the suspicious transaction reports, particularly in situations where online gambling platform are used across borders;
    - organising training sessions for staff and compliance officers, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments of their products/business model;
    - ensuring supervisory authorities provide clearer guidance on AML/CFT risks, customer due diligence and suspicious transaction reporting

requirements, and on how to identify the most relevant indicators to detect money laundering risks;
    - raising awareness of online gambling operators on emerging risks that may increase 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 and in cyber security, and to detect and prevent money laundering; in this regard, pooling resources with other Member States (such as organising joint training) could be considered.
- Member States are encouraged to require that supervisory competent authorities, where appropriate, 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 transactions).
- Member States should ensure that financial intelligence units provide feedback to online gambling operators about the quality of the suspicious transaction report and ways to improve the reporting, and about how the information provided in the report is used, preferably within a set period of time.
- Member States should develop standardised template(s) at EU level for suspicious transaction and suspicious activity reports, taking into account specific characteristics 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 customer due diligence requirements and data protection rules and on reporting.

2) For the sector:

- Member States should ensure that online gambling operators regular organise training sessions of the staff and compliance officers on a regular basis, focusing particularly on risks of infiltration or ownership by organised crime groups, and regularly reviewing risk assessments of their products/business model. Such training could be made mandatory for certain categories of staff at the appropriate level of detail for their position.
- Member States should ensure that online gambling operators promote systematic risk-based customer due diligence of the winners, and promoting a lower threshold of winnings subject to customer due diligence (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, if not done already.
- Member states could ensure that customers are not permitted to open multiple accounts with the same operator (and also prohibit transfers between customer accounts), unless the accounts are on different brands that operators can link to in the back end. If this rule is breached, the operator could reserve the right to block

and/or delete the extra account held by the player and to reallocate all the funds to a single account.

- Member States could also provide an obligation for the player's account name to match the name of the payment card or other payment methods used to deposit/withdraw funds, and ensure that the player's account is non-transferable, i.e. players are prohibited from selling, assigning, or transferring accounts to or acquiring accounts from other players.

3) For the Commission:

The Commission could provide guidance on Article 11(d) concerning the implementation of customer due diligence in case of 'several operations which appear to be linked'.

NON-PROFIT ORGANISATIONS

1. Collection and transfers of funds through a non-profit organisation (NPO)

Product

Collection and transfers of funds through a non-profit organisation

Sector

Non-profit organisations

General description of the sector and related product/activity concerned

NPOs can have a variety of legal forms, depending on the country in which they are established. The Financial Action Task Force (FATF) has adopted a functional definition of an NPO, therefore, which is used by the European Commission for the purposes of this supranational risk assessment (SNRA). **This definition is '**a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for

purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works".[109]

There is a wide range of NPO sub-sectors, including humanitarian aid, development assistance, sports, advocacy, etc.

For humanitarian NPOs, the objective is to save and preserve the lives of people affected by natural or man-made disasters, with full respect for international humanitarian law and for the principles of humanitarian action (neutrality, impartiality, humanity and independence[110]). Humanitarian NPOs may be active in and outside Europe, and in different operational contexts.

Much humanitarian aid is provided in areas experiencing armed conflict or other violence, or dealing with its consequences. Humanitarian organisations may also operate in regions and countries where people and entities designated as 'terrorist' are present and likely to be pursuing their activities. While the humanitarian aid sector accommodates a wide range of organisations with varying degrees of operational and organisational capacity, a large segment of NPOs receives institutional humanitarian aid funding, including from the EU and and from Member States in charge of managing EU funds. These are subject to a strict contractual framework with a high degree of safeguards.[111]

Description of the risk scenario[112]

- NPOs may be established, or existing NPOs used, to raise funds. Criminal funds are then sent to the NPOs, and:

  - complicit NPOs may intentionally support a terrorist group or criminal organisation;
  - legitimate NPOs may be exploited by outsiders;

[109] This definition is used in the Interpretative note to Recommendation 8: http://www.fatf-gafi.org/publications/fatfgeneral/documents/plenary-outcomes-june-2016.html#npo
It should be noted that there is no common EU legal definition of an NPO, and that their forms and definitions vary greatly at national level. The FATF, however, focuses on **service delivery organisations** and does not include expressive/advocacy NPOs within the scope of R8. R8 refers only to terrorism financing risks related to NPOs, and not money laundering risks.

[110] According to the humanitarian principle of impartiality, humanitarian aid must be provided solely on the basis of need, without discrimination between or within affected populations.

[111] EU humanitarian aid funding is managed by the European Commission and is channelled through partners, including NPOs, which are selected on the basis of specific legal, financial and operational criteria and which have signed a Framework Partnership Agreement (FPA). Donors and NPOs have the shared aim of ensuring that aid reaches those most in need and is not diverted elsewhere. While there is risk inherent in operating in environments where designated terrorist groups may have a presence, this risk stems from the operating environment itself, and not from the legal status of the operating entity.

[112] In line with international policy commitments taken by the Commission with a view to promoting greater effectiveness and efficiency, humanitarian assistance is increasingly delivered as cash transfers. This allows beneficiaries and their families to meet their most pressing needs with dignity and flexibility and introduces a sense of normality to their disrupted lives. Such cash transfers in humanitarian aid operations are not concerned by the present assessment.

- legitimate NPOs may be exploited by insiders.

- Criminals may use 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, and:

  - 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

In this risk assessment, NPOs are as defined in FATF Recommendation 8. The risk scenario covers the collection of funds by an NPO and transfers of funds from it to project partners/beneficiaries.

It must be emphasised that assessing the whole sector is a complex exercise on grounds of its overall diversity and because each NPO sub-sector involves a different level of risk/threat.

Since the assessment concerns money laundering and terrorist financing, which affects the internal market and cross-border activities, it applies to the collection and transfer of funds within the internal market and also to the collection of funds within the EU for transfer to third countries.

Threat

Terrorist financing

Assessment of the terrorist financing threat from the collection and transfer of funds by NPOs shows that this is not a method frequently used by terrorist groups. Looking at the the number of NPOs registered, very few are misused. In rare cases, however, NPOs may be infiltrated by terrorist groups, which may then represent a significant threat, in particular as concerns the funding of foreign terrorist fighters.

In general, the collection and transfer of funds through NPOs is regulated by various national, and sometimes regional, laws. Compliance with these laws requires some technical expertise and involves different levels of transparency and accountability processes. Due diligence procedures for NPO registration, licensing and access to financial services across the EU have become stringent. Terrorists who aim to finance terrorist activities under the guise of an NPO need to understand these procedures, and the requirements may deter them from using an NPO.

Some NPO activities may involve a higher risk when it comes to funding sources (unknown/cash/international sources/high-risk countries), types of activity or beneficiaries (unknown/high-risk countries/high-risk customers/use of informal channels

for sending money across borders). Risks increase when no formal banking channels are available for money transfers to and by NPOs. The main reasons for the use of informal money transfer systems are that banks are becoming increasingly unwilling to provide financial services to NPOs (a trend known as bank derisking) and a decline in correspondent banking. The risk, therefore, stems to some extent from financial exclusion. New technological tools such as crowdfunding and blockchain systems might be misused by the NPO sector, and regulators may need to assess and address any related risks. Conversely, these new tools could also be used to boost the traceability of funds.[113]

The work of humanitarian NPOs may take place in areas which are at times high risk and where non-state armed groups or individuals designated as terrorists are present. The specific risks depend on various factors, such as the level of professionalisation of an NPO and the situation in that particular country, including the political dynamics of the conflict in question.

Conclusions: The NPO landscape is very diverse. Although NPOs have been infiltrated only in very few cases and that generally more specific knowledge is needed to access funds collected or transferred by NPOs to finance terrorist activities 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 considered as less significant (level 1).

Money laundering

The assessment of the ML threat related to collection 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.[114]

Conclusions: In that context, the level of threat for ML is considered as moderately significant (level 2).

[113] Some charities and fundraising organisations specifically exploit Muslim communities for financial support under the guise of humanitarian aid, for instance to support families and orphans of 'martyrs', and to build mosques and wells. There is a high mobilisation potential for fundraising among jihadist sympathisers. In most cases, the calls for donations are made in mosques, via websites, web fora and crowdfunding platforms located in Europe, and provide little information on the end use of the funds, which are often withdrawn in cash. A few calls for donations explicitly requested that donations be made in Bitcoin.

[114] In a recent case, an organized criminal group (OCG) led by a catholic Church prelate officially resident in Rome whilst spending most of the time travelling worldwide offered ML to other OCGs: The prelate and his associates were able to offer to their "customers" charities' bank accounts as legal vehicle so as to move funds globally without raising suspicion. Italian authorities suspected the funds channelled through these bank accounts come from tax evasion, MTIC and VAT frauds, and serious crimes (such as drug trafficking).

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 less significant (level 1).

Vulnerability

Terrorist financing

The risk assessment of the terrorist financing vulnerability of the collection and transfers of funds by NPOs is set out below.

General remarks

Risk analysis of the NPO sector from a vulnerability perspective is difficult, given the diversity of the sector.

a) risk exposure

As mentioned above, some NPOs may be exposed to risks. Small amounts of funding are in cash, which makes it difficult for law enforcement agencies and financial intelligence units to trace the sources of funds and transfers sent abroad. Risks also increase when no formal banking channels are available for NPO money transfers. As was made clear earlier, informal money transfers are generally only used because banks are becoming increasingly unwilling to provide financial services to NPOs (a trend known as bank derisking) and because correspondent banking is declining. The risk, therefore, stems to some extent from financial exclusion.

The work of humanitarian NPOs may take place in areas which are at times high risk and where non-state armed groups or persons designated as terrorists are present. The specific risks depend on various factors, however, such as the level of professionalisation of an NPO and the situation in that particular country, including the political dynamics of the conflict in question.

b) risk awareness

Risk awareness is on the rise in the NPO sector. NPOs undertake their own risk assessments, which take account of the location, the type of activity, the organisation's past involvement in the area and relationships with other sectors. They are starting to develop controls and due diligence measures for the transfer and collection of funds (sanction lists, screening and criminal law reform have all helped). The sector is also developing peer-learning exchanges on due diligence practices, transparency and accountability issues and risk management, as well as awareness-raising on terrorist financing. NPOs (in particular humanitarian ones) are becoming more and more aware of risks, in particular where financial transactions take place outside the financial system. There is also greater collaboration and outreach to the banking sector to facilitate safe and regulated channels for legitimate humanitarian causes. This boosts transparency and helps safeguard NPOs from misuse by terrorists, while at the same time allowing humanitarian aid to be delivered to the regions most in need.

The sector is also engaged in self-regulation, with codes of conduct being developed by the fundraising and service delivery sectors, which often cover governance, reporting, monitoring of the use of funds, and principles such as 'know your donors' and 'know your beneficiaries'.

In response to donor requirements and to ensure that the aid reaches its intended beneficiaries, NPOs are increasingly investing in strong compliance and internal audit functions, as well as capacity building in relevant issues such as bribery and corruption countermeasures. NPOs receiving humanitarian aid funding from the EU and from Member States in charge of managing EU funds are subject to a strict contractual framework with a number of safeguards.

The NPO community is vitally important for providing humanitarian assistance around the world. To safeguard the legitimate objectives of such assistance, more information about terrorist financing risks may be needed within the NPO sector to improve risk awareness.

c) Legal framework and checks

The NPO sector is regulated at national and sometimes regional level (in civil law and tax law). There is no centralised organisational framework and the rules are not harmonised at EU level. NPOs are not directly included in the anti-money laundering/counter terrorist financing (AML/CFT) framework at EU level, but are included indirectly via the obligations of entities that have NPOs as clients, and via Member States' obligations concerning beneficial ownership structures. Conditions for the registration and operation of NPOs differ from country to country. Competent authorities tend to the view that existing checks on the collection and transfer of funds within the EU are quite robust. Some weaknesses were reported, however, concerning the transfer of funds outside the EU.

Beyond AML/CFT requirements, humanitarian NPOs are governed by the principles of humanity, impartiality, neutrality and independence. In addition, specific categories of humanitarian NPOs, particularly those that have been assessed by the European Commission, are subject to ongoing checks during the lifetime of the partnership and the specific humanitarian actions. These checks, which include detailed reporting on actions, obligations on record keeping, and regular audits both at HQ and in the field, go beyond the strict eligibility and suitability criteria which are checked through a detailed selection process prior to the signature of the FPA.

In almost all Member States, NPOs are subject to some kind of state supervision, be it by tax authorities, charity regulators or other types of supervising authority. On the legal framework, a balance needs to be found between the counter-terrorism agenda and the legitimate objectives of humanitarian NPOs.[115]

[115] For example, the preamble to 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 an exemption for humanitarian activities by impartial humanitarian organisations.

Conclusions: the risk exposure of the NPOs is impacted by the intrinsic nature of their activities, and various degree of risk awareness exist. The applicable legal and tax frameworks and national practices are diverse but appear to provide controls and checks while the specific setup of the humanitarian sector described above should be acknowledged. In that context, the level of TF vulnerability is considered as moderately significant (level 2).

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 considered as less significant (level 1).

Money laundering

The assessment of the ML threat related to the collection and transfers of funds through NPOs has been considered in conjunction with TF schemes related to the collection 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 moderately significant (level 2).

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 also considered as less significant (level 1).

Mitigating measures

1) For the Commission

- Continue to engage with NPOs that receive EU funding on the relevant EU legal framework, as well as on how to identify risks and meet due diligence requirements.
- Continue to take part in multi-stakeholder exchanges involving all professional sectors, in particular the financial sector, involved in business with NPOs.
- Continue to engage with and provide guidance to humanitarian NPOs in receipt of EU funding on the risks of ML/TF and due diligence requirements, taking into account the best practices of huminatarian organisations.

2) For competent authorities

- Member States should ensure better NPO involvement in national risk assessments and in developing information and awareness programs designed to counteract the risk of abuse, and should support NPOs by providing awareness-raising materials for NPOs (at Member State level as well as EU level).
- Member States should also further analyse the risks faced by the NPO sector.

PROFESSIONAL SPORTS

1. Investments in professional football and transfer agreements relating to professional football players

Product
Investments in, and transfer agreements relating to, professional football players

Sector
Professional sports

General description of the sector and related product/activity concerned

The sporting industry is one of many sectors that could be attractive for criminals for money laundering purposes and merits closer consideration given its social and cultural impact, the large scale of monetary transactions, and the increase in the number of individuals involved.

Like many other businesses, sport and gambling have been used by criminals to launder money and derive illegal income. As in the art world, criminals in the sports world are not always motivated by economic gain. Social prestige, appearing with celebrities, and the prospect of dealing with authority figures may also attract private investors with dubious intentions.

Description of the sector

Football is played by more than 265 million people in the world. According to the Fédération Internationale de Football Association (FIFA), there are 38 million professional players, duly registered, and about 301,000 clubs. Football has seen extraordinary growth since the early 1990s, a result of increased television rights and sponsorships. The market for professional players has experienced an unprecedented internationalisation, allowing ever-greater transfers of resources across continents.

In football, image contracts, advertising contracts, and sponsorship contracts can be tools for criminal practice, notably tax evasion, since the money stipulated in these contracts is commonly transferred to accounts belonging to companies in third countries. This results in a serious risk of fraud, since it is easy to avoid declaring the money received, even if this requires the use of third parties in various financial transactions.

The most common form of cash payments involves jurisdictions located abroad that allow the final destination of payments to be disguised. Image rights are also used to conceal the amounts actually paid to players.

In addition, gambling is directly linked to football through betting on games and matches.

Relevant actors

Football is administered by FIFA, which is based in Zurich, Switzerland. It is a private entity, governed by Swiss law, controlling the whole world of football through a confederation system. It has the authority to promote and develop football globally. Each country has an associate that must follow FIFA's rules and laws. FIFA has a clear responsibility to safeguard the reputation and integrity of the sports sector.

For this reason, FIFA approved the Code of Ethics in 2004 (later revised on several occasions),[116] which enabled the creation of the new Ethics Committee, of which it is a key member. As part of its work to strengthen ethics in sport, FIFA offers technical support through the Early Warning Systems GmbH company, founded specifically to monitor sports betting and to prevent negative effects of unethical behaviour in football games.

As a supervisory body that monitors the football sector closely, including its management of clubs that often bear debts incompatible with effective financial capacity, FIFA includes six confederations: Asian Football Confederation in Asia and Australia (AFC), Confédération Africaine de Football (CAF), Confederation of North, Central American and Caribbean Association Football (CONCACAF), Confederation Sudamericana de Fútbol (CONMEBOL), Oceania Football Confederation (OFC), and Union of European Football Associations (UEFA). UEFA is by far the largest of the six continental confederations.

[116] From 12 August 2018 FIFA's new Code of Ethics (CoE) has come into force.

FIFA relies on the Transfer Matching System (TMS) for obtaining information on the international transfer of players, which was previously restricted to business stakeholders. Through this system, more than 30 types of information are recorded online, such as player history, clubs involved in the business, payments, values, contracts, and other kinds of information.

The national associations have a responsibility to discipline, coordinate, and administer football in their respective countries. These national organisations are considered the key regulators in their countries, but they must still comply with specific regulations set by FIFA. In turn, the national associations may be subdivided into regional bodies. Clubs are considered cells that are at the base of each regional body.

Over the course of FIFA's history, its statutes have been submitted to several reviews, which have allowed the statutes to modernise and transform into an increasingly comprehensive body of work. They determine the basic laws of international football, including numerous rules about competitions, transfers, illegal drug use, and a variety of other subjects. These bylaws were approved at the 59th FIFA Congress in Nassau, Bahamas, on June 3, 2009, and became effective on August 2 of the same year. Changes to the FIFA statutes can only be made by a Congressional session and require a 75% majority of national federations present and entitled to vote. This makes FIFA statutes and their implementing regulations equivalent to a constitution of the governing body of international football.

Description of the risk scenario

The first document from the EU that recognised the importance of the sport was published in July 2007 (EU White Paper on Sport).[117] It states that, 'sport is confronted with new threats and challenges, as commercial pressures, exploitation of young players, doping, corruption, racism, illegal gambling, violence, money laundering, and other activities detrimental to the sport'. Many factors have led to the use of illegal resources in football, not least its complex organisation and insufficient transparency.

In March 2013, the European Parliament adopted a resolution on match-fixing and corruption in sport.[118] This was followed by a resolution on 11 June 2015 on revelations on high-level corruption cases in FIFA[119] and a resolution on 2 February 2017 on an integrated approach to sport policy, covering good governance, accessibility and integrity.[120] During the plenary session in July 2016, the CULT committee tabled an oral question to the Commission on match-fixing, asking for a full commitment to ratifying

[117] *White Paper on Sport*; European Commission, Brussels, 11.7.2007; COM(2007) 391 final.
[118] European Parliament resolution of 14 March 2013 on match-fixing and corruption in sport (2013/2567(RSP)). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52007DC0391
[119] European Parliament resolution of 11 June 2015 on recent revelations on high-level corruption cases in FIFA (2015/2730(RSP)). Available at: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0233+0+DOC+XML+V0//EN
[120] European Parliament resolution of 2 February 2017 on an integrated approach to Sport Policy: good governance, accessibility and integrity. Available at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0012

the Council of Europe Convention on the Manipulation of Sports Competitions.[121] The Commissioner's answer underlined the Commission's support for the Convention as a valuable tool in the fight against match-fixing, as it represents a solid basis for ensuring pan-European coordination and cooperation in that fight. However, cooperation between Member States and institutions is needed to ensure that the Convention enters into force in the EU.

Social status is also a factor driving attraction, and results in the investment of great sums of money with no apparent or explicable financial return or gain, other than the social prestige of investing in professional sport. Professional sport's popularity, and especially that of professional football, can be a tool for criminals to legitimise themselves by appearing alongside famous people, entrepreneurs, or authorities.

Football is a highly relevant candidate for study because of its rapid transformation from a popular sport to a global industry with significant economic impact. Given its social importance, it has been a vehicle for the transmission of cultural and universal values.

Many cases have shown that the football industry has featured illegal practices, including money laundering, corruption, and drugs.

Lack of transparency regarding the transfer of players and the true owners or managers of football clubs, can lead to the industry being dominated by a handful of people and cause serious concern about prevention and suppression of money laundering.

Also, the use of nonfinancial professionals, such as family members, lawyers, consultants, and accountants as a means of creating structures to move illicit funds has also been observed by the Financial Action Task Force (FATF). The money stipulated in such image contracts (for exploitation of a player's personal appearance as part of an extensive advertising campaign) is often transferred to accounts of companies in third countries with serious risks of fraud. Advertising and sponsorship contracts can also be used for money laundering. Organized crime could sponsor sport and constitute a bridge to legitimate business. The most common form of payments involves jurisdictions located abroad, always as a way to hide the last destination.

Furthermore, FIFA data are neither public not easy to obtain, and non-Swiss authorities would be forced to request international legal cooperation to access them because FIFA is headquartered in Switzerland.

Threat

Terrorist financing

[121] The **Convention on the Manipulation of Sports Competitions (the Macolin Convention)** was opened for signature on 18 September 2014, at the 13th Council of Europe Conference of Ministers responsible for Sport in Macolin, Switzerland: https://www.coe.int/en/web/sport/about-the-convention-on-the-manipulation-of-sports-competitions

The assessment of the terrorist financing (TF) threat arising from collecting and transfering funds in the football sector shows that this method of funding terrorism is not frequently used by terrorist groups. Indeed, no known cases of TF from money moved through the football sector exist.

Conclusion: Given this context, the level of terrorist financing threat related to football is considered moderately significant (level 2).

Money laundering

In some Member States, authorities are investigating football clubs amid concerns the sector is being used to launder dirty cash and clubs are underreporting suspicious behaviour.[122]

Methods

The methods through which organised criminal groups operate can be illustrated through several recent examples:

- In May 2016, during Operation *Matrioskas*, the Portuguese Police (Polícia Judiciária), supported by Europol, dismantled a transnational organised criminal group mainly composed of Russian citizens who focused on money laundering through the football sector. Active since at least 2008, this criminal network is thought to be a cell of an important Russian mafia group, directly responsible for laundering several million euros across numerous EU countries, most of it believed to derive from polycriminal activities committed outside the EU area.

  The group's known *modus operandi* was to identify EU football clubs in financial distress, then infiltrate them with benefactors who provide much needed short-term donations or investments.

  After gaining trust through donating, these same benefactors orchestrate the purchase of the clubs. The purchase of such clubs is facilitated by individuals operating as front men for opaque and sophisticated networks of holding companies, invariably owned by shell companies registered offshore and in high-risk third countries. As a result, the real owners and those who ultimately control the club remain unidentified, as does the true origin of the funds used to purchase them.

  Once clubs are under the control of the Russian mafia, the large scale of financial transactions, cross-border money flow, and shortcomings in governance allow them to be used to launder dirty money (usually via the over- or under-valuation of players on the transfer market and on television rights deals) and for betting activities (both for the generation of illegal proceeds due to match fixing or for pure money laundering purposes). Using this method, the criminal group first made a series of

[122] https://kyc360.com/news/uk-football-clubs-in-live-money-laundering-investigations/

donations to and investments in a club which had competed in the main Portuguese football league until it faced financial difficulties in 2012 that saw it relegated to lower divisions. In July 2015, the group then purchased the club.

The police investigation started due to the detection of strong red flag indicators against the suspects. In particular, suspicion was raised by the high standard of living the suspects enjoyed while using high value assets registered in the names of third parties (use of frontmen). They imported large amounts of cash from Russia to Portugal, in violation of EU cash regulations (use of cash couriers), and they created and used opaque networks of offshore shell companies intended to preserve the identities of their owners.

Since July 2015, significant evidence has been gathered showing that this criminal group operates as a criminal association conducting money laundering, tax fraud, corruption and forgery of documents while preparing various transnational criminal offences.

- European football clubs acquired by criminal organisations can be further used to launder money through betting activities in fixed football matches.
- Sports corruption and match-fixing are often carried out by criminal networks with links to drug trafficking, illicit tobacco smuggling, and burglaries.
- An organised crime group had created different websites as part of an online betting platform used to place bets on manipulated sport events that took place in multiple European countries. The criminals are suspected of being involved in attempts to fix professional football matches in Serbia, North Macedonia and Czechia, among other countries. The organised criminal group behind these activities has previously gambled primarily on the Asian market, where they were guaranteed considerable financial gains by knowing the end result of the matches. The ring developed synergies with other major criminal groups in different countries, in order to invest money gained from other serious crimes, including drug trafficking.

<u>Conclusions</u>: Given this context, the level of money-laundering threat related to football is considered significant (level 3).

Vulnerability

Terrorist financing

The assessment of the TF vulnerability related to professional football shows that:

a) risk exposure

As set out above, there is an inherent risk for football clubs and football-related activities where 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 the perspectives of law enforcement authorities and FIUs.

b) risk awareness

The football sector has a centralised organisational framework but the rules applicable to it are not harmonised at EU level and vary from one Member State to another. The sector's centralised organisation appears limited with regard to the authorities' ability to provide effective guidance or assistance. Risk awareness is increasing in the sector.

c) legal framework and controls

The sector is not included in the AML/CFT framework at EU level. Coverage by AML/CFT rules is left to Member States' discretion. The existing AML/CFT requirements are not necessarily considered adequate to address the sector's specific needs and the checks in place vary depending on the Member State.

Conclusion: Given this context, the level of terrorist financing vulnerability related to professional football is considered as moderately significant/significant (level 2/3).

Money laundering

The assessment of the money laundering vulnerability related to professional football shows that:

a) risk exposure

FIFA's attempt to obtain information through the Transfer Matching System has been to date effective but is not enough. It is a vital tool for obtaining information about the international transfer of players, previously restricted to only business stakeholders. But efforts by FIFA, which sometimes focus on purely commercial and private interests, should not replace the work of authorities.

Certain obligations should be established, like requiring clubs, federations, and confederations – and those who provide advisory, auditing, bookkeeping, and consulting in this area – to communicate suspicious transactions to the Financial Intelligence Units. Clubs, according to the FATF, are deliberately being used to launder money, and thus more must be done. FIFA data are not public and difficult to obtain, and therefore authorities will be forced to request international legal cooperation to access the data, because FIFA is headquartered in Switzerland.

b) risk awareness

In addition to the importance of collecting information, it is essential for authorities to track down the assets obtained from criminal activities in sport and gambling.

FIFA's efforts alone are not enough to prevent unlawful practices. Associations, federations, and confederations must engage and establish proper references or guidelines within football, and provide the necessary support to clubs through professional training in order to facilitate suspicious transaction reports.

c) legal framework and controls

The principle of confidentiality cannot be invoked to neglect reporting suspicious activities, following FATF Recommendation No. 9. Indeed, the duty of professionals not

connected with the financial sector to report, also set out in FATF Recommendations Nos. 18, 21, and 22, is an essential tool to combat misuse of good practices by managers in hiring players. The legislation that advocates for autonomy in the organisation and functioning of sports bodies must also require effective financial and administrative transparency and set out the civil and criminal liabilities of its directors.

Conclusion: the sector is currently vulnerable to money laundering. While the sector's level of awareness of the risks of money laundering seems higher than for terrorist financing, the sector's ability to provide for dedicated resources and training in this area is still quite low. The legal framework in place has increased the checks applied in the sector, but these remain inadequate. In that context, the level of money laundering vulnerability in the professional football sector is considered moderately significant/ significant (level 2/3).

Mitigating measures

The European Parliament has urged Member States to create the crime of sporting fraud.[123] In addition, in 2014, the FIFA Executive Committee approved the Regulations on Working With Intermediaries.[124]

The Annex to the Commission Decision adopting the Arrangement for Cooperation between the European Commission and the Union of the European Football Associations (UEFA),[125] explicitly refers to the ambition of both signatories to prevent the football sector from being used for money laundering purposes. UEFA has committed to engaging with this process to help the Commission to assess the money laundering risks in the football sector.

Member States should also consider, among other things:

- determining how players' agents (including individuals or legal entities that promote, mediate, trade, hire, or negotiate athletes' transfer rights) are required to report suspicious operations. Individuals, corporations, associations, federations, confederations, and clubs that are involved in the promotion, brokerage, marketing, or trading of athletes should also be covered by this requirement in relation to negotiations;
- requiring football clubs to keep records of every contract and related mediation contracts for at least 5 years;
- requiring full identification of investors, even when corporations in the country represent them;

[123] European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report) (2013/2107(INI)); OJ C 208, 10.6.2016, p. 89–116. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013IP0444

[124] https://www.fifa.com/about-fifa/who-we-are/news/fifa-executive-committee-approves-regulations-working-with-intermediarie-2301236

[125] European Commission, Brussels, 19.2.2018, C(2018) 876 final.

- applying more requirements for control and registry of the origin of the account holders and the beneficiaries of the money that is remitted to tax heavens. Further mechanisms should be designed in order to try to get third countries to provide all information, in a timely manner, when requested;
- offering training to clubs and transfer agents in federations, confederations, and any other supervisory body, with the aim of strengthening their roles;
- requiring clubs, federations, and confederations to comply, under penalty of sanctions, with the Registration of National or International Players Transfers. They must provide complete information about the transaction, by detailing its financial structuring and attach the agent's contract and proof of identity of the agent and the player to the transfer agreement between buyers and sellers;
- creating an obligation to conduct an independent audit in sports federations and confederations.

Specifically as regards agents, Member States should:

- require those who act as agents of athletes, even relatives or lawyers, to obtain a licence to avoid the lack of transparency of their activities;
- regulate the legal framework for football agents to include all trading beyond the clubs;
- require players' agents to be licensed, so as to increase transparency in their dealings;
- regulate and supervise all activities by players' agents, ensuring they have the required licencing or authorisation;
- establish legal limitations on doing business as a player's agent, requiring agents to be registered, with a detailed résumé, in a regulatory agency in addition to FIFA;
- bar all those with criminal convictions or those who have lost civil cases relating to fraud, tax evasion, or other civil liabilities, at state, municipal, or federal levels;
- require agents to inform all customers as to their contractors.

FREE-TRADE ZONES

1. Free ports

Product

Free ports

Sector

Free-trade zones, Free zones — Customs, direct taxation

General description of the sector and related product/activity concerned

Free-trade zones (FTZs) are a type of special economic zone (SEZ), i.e. an area in which business and trade laws differ from those in the rest of the country. In an FTZ or in a SEZ goods can be landed, stored, handled, manufactured or reconfigured and re-exported under specific customs regulation and generally without being subject to customs duty. FTZs are normally organised around major seaports, international airports and national frontiers — areas with many geographical advantages for trade.

FTZs are also known as **free zones,** a customs arrangement used widely around the world to facilitate trade. They are provided for in the Kyoto Convention (Specific Annex D), to which the EU and 115 other parties are signatories. The 1999 Revised Kyoto Convention defines them as 'a part of the territory of a contracting party where any goods introduced are generally regarded, insofar as import duties and taxes are concerned, as being outside the customs territory'.

The Union Customs Code (UCC) also makes provision for free zones.[126] An EU Member State can designate part of its customs territory as a free zone. Free zones have to be enclosed, and the perimeter and entry/exit points must be subject to customs supervision. Their creation requires prior approval from the customs authorities, who must be notified in advance of the activities to be carried out and may impose prohibitions or restrictions.

In free zones, Member States can apply:

- reliefs and exemptions from VAT and excise duties, subject to specific rules under EU legislation on indirect taxation; and
- such direct taxation arrangements as they consider appropriate, subject to:
    - EU State-aid rules (which apply to free zones in general); and

[126] Article 243 of Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code (OJ L 269, 10.10.2013, p. 1).

- the code of conduct on business taxation[127] (which they have agreed to apply to limit harmful tax practices).

Description of the sector

Free ports are warehouses in free zones that were originally intended as spaces to store merchandise in transit. They have become popular for the storage of substitute assets, including art, precious stones, antiques, gold and wine — often on a permanent basis. Apart from secure storage, they offer the deferral of import duties and indirect taxes such as VAT or user taxes, and a high degree of secrecy.

In 2016, warehousing accounted for 30% of global FTZ activities, with stored goods worth an estimated $536 billion.[128]

In the EU:

There are 82 free zones in the EU.[129] The only free port (i.e. FTZ specialising in the storage of high-value luxury goods) is the Luxembourg Freeport, which was inaugurated in September 2014 and has only five counterparts elsewhere in the world: in Geneva, Monaco, Singapore, Beijing and Delaware (USA).

The other free zones are located in 22 Member States. They fall into various SEZ categories, are approved by the Commission and are mainly used as logistics and trade hubs, not specifically for wealth management purposes or storing luxury goods.

Description of the risk scenario

FTZs continue to pose a counterfeiting threat, as they allow counterfeiters to land consignments, adapt or otherwise tamper with loads or associated paperwork and then re-export the products without customs intervention, and thus to disguise the true origin and nature of the goods, and the identity of the original supplier.

Currently, there are an estimated 3,500 free zones and SEZs around the world. FTZs do not service maritime traffic only – many are located at international airports and national frontiers, from where goods can be transported overland.

Weaknesses continue to be found in several FTZs and some have been used in a series of organised crimes, including:

- narcotics trafficking;

[127] The Code of Conduct Group (Business Taxation) was set up by Ecofin on 9 March 1998. Its main function is to assess tax measures that fall within the scope of the December 1997 code of conduct on business taxation and to oversee the provision of information on those measures.
[128] https://www.cps.org.uk/files/reports/original/161114094336-TheFreePortsOpportunity.pdf
[129] Free zones which are in operation in the customs territory of the Union, as communicated by the Member States to the Commission:
https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/customs/procedural_aspects/imports/free_zones/list_freezones.pdf

- the illegal ivory trade;
- people-smuggling; and
- counterfeiting.

Organised criminal gangs (OCGs) misusing FTZs are often poly-criminal, e.g. the operations of OCGs engaged in intellectual property rights (IPR) crime often entail VAT fraud, corruption and money-laundering.

Legal businesses owned by criminals remain key to money-laundering activities. They enable trade-based schemes that do not often involve the physical movement of cash and provide a front for money transfers.

In most EU free ports and customs warehouses (with the exception of the Luxembourg Freeport), precise information on the ultimate beneficial owners (UBOs) of goods is not available. The 5th Anti-Money-Laundering Directive (AMLD5) explicitly covers free port operators and other actors in the art market, as they will be 'obliged non-financial entities' from 10 January 2020 onwards and therefore subject to the same customer due diligence (CDD) requirements as, for example, real-estate agents and notaries. They will also take on the role of anti-money laundering (AML) gatekeepers, as they will have to report suspicious transactions to financial intelligence units (FIUs).

The value of the goods stored in free ports is estimated to be in the billions of euros. Due to privacy and confidentiality clauses (akin to bank secrecy), owners of free ports do not disclose the value of goods stored on their premises, as declared by customers, so it is difficult to give a precise estimate.

To use Swiss free ports as a guide, in September 2012 *The Economist* estimated that free ports in Geneva and Zurich held 'well over $10 billion worth of paintings, sculptures, gold, carpets and other items'.[130] In 2016, the Swiss government estimated that the country's free ports held around EUR 100 billion in valuables.[131]

Threat

The Financial Action Task Force (FATF) considers that FTZs such as free ports boost economic opportunities, but lack effective law enforcement and regulatory oversight.[132]

Free ports are perceived as facilities that protect their clients' identity and financial dealings, much as private banks used to. They have been described as institutions that are

[130] https://www.economist.com/finance-and-economics/2012/09/01/paint-threshold
[131] https://www.finews.com/news/english-news/23238-swiss-freeports-move-to-crack-down-on-art,-loot
[132] *Money-laundering vulnerabilities of free-trade zones*: http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf

exempt from the duty of collecting and reporting valuable data relating to potential cases of tax evasion, corruption and money laundering.[133]

Terrorist financing

Free ports operate several restrictions that prevent local authorities from investigating property stored at their premises.

Recent case illustrating the *modus operandi*:

In December 2016, the Swiss authorities seized cultural relics that had been looted from Syria, Libya and Yemen, and were being stored in Geneva's free ports, which provide highly secure warehouses where items can be stored tax-free. The looters had brought the confiscated objects to Switzerland via Qatar. Three of the pieces were from the ancient city of Palmyra (Syria), a UNESCO world heritage site systematically destroyed by the ISIL (Da'esh) jihadists who had seized it in May 2015.

Conclusions: The TF threat relating to free ports is considered significant (level 3).

Money-laundering

EU-based criminals rely predominantly on manufacturers based abroad and then organise the importation, transportation, storage and distribution of counterfeit goods in the EU. However, some are also active manufacturers of counterfeit goods in the EU. Such manufacture is facilitated by the use of fake labels and packaging imported from outside the EU and is often orchestrated by OCGs; there are indications that such criminality is on the rise.

OCGs involved in excise fraud rely heavily on the use of legal business structures. This involves:

- setting up front companies;
- colluding with key employees in customs and bonded warehouses; and
- cooperating with transport companies and distributors.

Recent cases illustrating the *modus operandi*:

1. In 2015, the Panama Papers leak revealed that David Nahmad, a prominent private art collector, was the ultimate owner of a Modigliani painting, *Seated man with a cane*. Nahmad had acquired the artwork at a Christie's auction in 1996 for an estimated $25 million through his International Art Center (IAC) in Panama and stored it at the Geneva Freeport.

   The painting attracted public attention when the grandson of Oscar Stettiner, a Jewish antiques dealer, claimed that the Nazis had looted it during the occupation of Paris

[133] http://www.taxjustice.net/wp-content/uploads/2013/04/TJN-141124-CRS-AIE-End-of-Banking-Secrecy.pdf

in 1939. The Swiss authorities initially seized it, but later returned it to Nahmad when the claimant was unable to prove ownership, as the description of the artwork that had been used to back the claim was too vague.

2. An October 2013 FATF report on *Money-laundering and terrorist financing through trade in diamonds* describes how criminals use diamonds as a form of currency to make their transactions more difficult to trace.[134]

   The report gives an example of a €800 million diamond fraud case perpetrated in the Geneva Freeport in 2005. An Antwerp-based courier business used the Freeport to smuggle precious stones, which it later sold on the Antwerp black market via offshore shell companies

Conclusions: The ML threat relating to free ports is considered significant (level 3).

Vulnerability

Terrorist financing

The assessment of TF vulnerability relating to free ports shows that:

a) risk exposure

Free ports are conducive to secrecy. With their preferential treatment, they resemble offshore financial centres, offering a high degree of security and discretion, and permitting transactions without attracting the attention of regulators or direct tax authorities. While a declaration of value is needed for goods stored in a free port or customs warehouse, this generally takes the form of a self-declaration by the owner or a representative and in most cases is not checked.

Goods held in free ports or under customs warehousing procedures are technically 'in transit', even though there are no time limits in most free ports of this kind. Goods can enter a free port, stay there indefinitely (while gaining in value) and be traded an unlimited number of times without ever being taxed.

In addition to confidentiality, the high value of monetary transactions, the law enforcement agencies' (LEAs') unfamiliarity with values and the portable nature of art all make the art market a suitable vehicle for illegal activity using free ports. As other ML techniques come under closer scrutiny, it has been suggested that smugglers, drug traffickers and arms dealers are increasingly turning to the art market.

b) risk awareness

As of 10 January 2020, free port operators and other actors in the arts market, such as auction houses and galleries, will become 'obliged non-financial entities' under the AMLD5. As AML gatekeepers, they will have to report suspicious transactions to FIUs and carry out CDD research in order to identify the UBOs of stored goods.

Following the 'Bouvier affair',[135] the national authorities unilaterally decided to apply AML requirements to the Luxembourg Freeport, but the operators had to be given a

[134] http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf

grace period of one year to update their files and align their procedures with the new requirements. This shows that risk awareness is still developing and that implementing the new measures may require significant work on the part of licensed operators to adapt their practices so that they can determine the UBOs of the goods brought in by their clients.

c) legal framework and controls

As they are subject to EU and national AML regulations, free ports are more highly regulated in the EU than elsewhere.

The main area in which free ports' arrangements vary is their information disclosure policies – local regulations are more burdensome in some locations than others in this respect.

Conclusions: When used anonymously, free ports are inherently exposed to TF vulnerability. Awareness in the sector is growing, but is still not sufficient. The level of TF vulnerability relating to free ports is therefore considered significant (level 3).

Money laundering

ML vulnerability is not assessed separately, but on the basis of the inherent factors described above. Nevertheless, the high incidence of corruption, tax evasion, criminal activity and ML cases detected and addressed by LEAs calls for specific consideration.

Conclusions: Free ports are inherently exposed to ML vulnerability when used anonymously. While the sector's awareness of ML risk seems higher than for TF, its structure and its capacity to provide dedicated resources and training are deficient. The level of ML vulnerability relating to free ports is therefore considered very significant (level 4).

Mitigating measures

There is scope to improve the regulation of EU free ports.

To avoid confusion, the Commission should address the following terminological inconsistencies in AMLD5 and the Union Customs Code (UCC):

- AMLD5 mentions free ports explicitly, but the UCC covers them only as a type of free zone; and
- in the UCC, the free zone procedure is on an almost equal legal footing with customs warehousing. This raises the question as to whether customs and bonded warehouses are (or should be) within the scope of the AMLD. As the market for customs warehousing is much larger than that for free ports, this issue should be clarified well before AMLD5 is due to be transposed (January 2020).

The Member States should:

[135] https://www.newyorker.com/magazine/2016/02/08/the-bouvier-affair

- carry out regular independent AML audits of agreed free zone operators' (AFZOs') compliance functions and ensure adequate and consistent enforcement of the AML procedures and oversight already enshrined in law;
- ensure that AFZOs regularly share information with the relevant AML authorities on UBOs and changes in the ownership of free port assets;
- place a reasonable, business-appropriate time limit on storing goods at free ports; and
- encourage the European art market, as one of the main customers of free ports, to self-regulate and improve its transparency, especially as art transactions continue to carry high ML risk due to their opacity and the subjectivity of asset evaluations.

CITIZENSHIP/RESIDENCE

1. Citizenship investment programmes and investor residence schemes

Product
'Golden visas' and 'golden passports'

Sector
Citizenship/residence

General description of the sector and related product/activity concerned

Recent years have seen a growing trend in investor citizenship and investor residence schemes. These aim to attract investment in a particular country by granting investors citizenship or residence rights there. Such schemes have raised concerns about certain inherent risks, in particular as regards security, money laundering, tax evasion/avoidance,[136] and corruption.

Investor citizenship schemes are often referred to as CIPs ('citizenship investment programmes'), 'citizenships for sale' or 'golden passports'. They allow foreigners to be naturalised as a citizen of a country in return for an investment, provided certain criteria are fulfilled. Investor citizenship schemes differ from investor residence ('golden visa') schemes, which aim to attract investment in exchange for residence rights in the country concerned.

Whilst the basis of these programmes is legitimate economic enrichment and diversification for the host nation,[137] there are reported instances of their abuse..

[136] Possible abuses are for example tax evasion through the abuse of dual residency and tax avoidance – setting up a company without physical presence to take advantage of tax incentives and low residence requirements of the investor scheme/citizenship Member State.
[137] The first CIP was created by St Kitts and Nevis in 1984 as a means to reinvigorate the economy. Its success prompted many other nations to follow suit.

As with gaining any second nationality, the benefits include ease of travel, residency and doing business. It might also be a means to moving assets outside of their country of origin, particularly if they live in an unstable political or economic climate, or if their wealth is ill-gotten. These schemes may also be used to avoid being prosecuted or convicted in their countries of origin. Many CIP nations are offshore financial centres whose structures provide security, secrecy and tax benefits. They may also offer individuals greater freedom in transacting in and with global financial centres, given the participant's (acquired) status as a local, who is therefore subject to less scrutiny.

Description of the sector within the EU

In the EU, three Member States (Bulgaria, Cyprus, and Malta) operate **investor citizenship schemes,** where citizenship is granted under less stringent conditions than under ordinary naturalisation regimes, in particular without effective prior residence in the country concerned.[138] Such schemes have implications for the European Union as a whole, as every person holding the nationality of a Member State is at the same time an EU citizen. Indeed, although these are national schemes, they are deliberately marketed and often explicitly advertised as a means of acquiring EU citizenship, together with all the rights and privileges associated with it, including in particular the right to free movement.

Investor residence schemes exist in 20 EU Member States:[139] Bulgaria, Czechia, Estonia, Ireland, Greece, Spain, France, Croatia, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia and the United Kingdom. The risks inherent in such schemes are similar to those raised by investor citizenship schemes. Furthermore, these schemes have an impact on other Member States as a valid residence permit grants certain rights to third-country nationals to travel freely, in particular in the Schengen area.

The European Parliament, in its Resolution of 16 January 2014,[140] expressed concern that national schemes involving the 'direct or indirect outright sale' of EU citizenship undermined its very concept. It called on the Commission to assess the various national citizenship schemes in the light of European values and the letter and spirit of EU legislation and practice.

In its 2017 citizenship report,[141] the Commission announced a report on national schemes granting EU citizenship to investors. The report described the Commission's action in this area and examined current national law and practices, while providing some guidance for Member States. To prepare the report, the Commission commissioned a

[138] Investors are required to invest between €800,000 and €2 million.
[139] The two lists overlap, as three countries — Bulgaria, Cyprus and Malta — trade with both.
[140] European Parliament Resolution of 16 January 2014 on EU citizenship for sale (2013/2995(RSP)): http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0038&language=EN&ring=P7-RC-2014-0015
[141] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Strengthening Citizens' Rights in a Union of Democratic Change: EU Citizenship Report 2017* (COM(2017) 030 final). Available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51132

study on legislation and practice pertaining to citizenship and residence schemes in all relevant Member States[142] and organised a consultation with Member States. The report also takes into account other relevant sources, including recent publications on the topic,[143] and was published in January 2019.[144]

Following the publication of the report, the Commission has set up a group of experts from Member States to look into the specific risks that arise from investor citizenship schemes and to address the aspects of transparency and good governance with regard to the implementation of both investor citizenship and residence schemes. By the end of 2019, the group of experts is expected to develop a common set of security checks for investor citizenship schemes, including specific risk management processes that take into account security, money laundering, tax evasion and corruption risks.

Threat

Third-country nationals may invest in a Member State for legitimate reasons,[145] but may also be pursuing illegitimate ends such as evading law enforcement investigation and prosecution in their home country, or protecting their assets from freezing and confiscation measures. Hence investor citizenship and residence schemes create a range of risks for Member States and for the EU as a whole: in particular, risks to security, including the possibility of infiltration of non-EU organised crime groups, as well as risks of money laundering, corruption and tax evasion. Such risks are exacerbated by the cross-border rights associated with EU citizenship or residence in a Member State.

There is also a concern about lack of transparency and governance of the schemes. Both citizenship and residence schemes have come under close public scrutiny following allegations of abuse and corruption linked to them in some Member States.[146] Furthermore, the procedure for screening applicants is often outsourced to private companies, and where there is a permanent risk of conflict of interest and corruption. Enhancing transparency and putting in place adequate risk management, control systems, and oversight mechanisms could help mitigate as far as possible some of these concerns.

---

[142] Fact finding study. Milieu Law and Policy Consulting, *Factual Analysis of Member States' Investor Schemes granting citizenship or residence to third-country nationals investing in the said Member State*, Brussels 2018.

[143] See in particular, European Parliamentary Research Service, *Citizenship and residency by investment schemes in the EU: State of play, issues and impacts*, October 2018.
http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)627128
Transparency International/Global Witness, *European Getaway — Inside the Murky World of Golden Visas*, October 2018, https://www.transparency.org/whatwedo/publication/golden_visas

[144] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Investor Citizenship and Residence Schemes in the European Union* COM(2019) 12 final.
https://ec.europa.eu/info/sites/info/files/com_2019_12_final_report.pdf

[145] Under Article 63 TFEU, the principle of free movement of capital applies between Member States and between Member States and third countries. Article 65 permits the free movement of capital to be restricted, in particular for reasons linked to public policy, public security or taxation.

[146] For example, in 2009, an Austrian politician told a potential Russian investor that he could have Austrian citizenship in exchange for an investment of €5 million and a donation to his party. A detailed account of reports of abuse or misuse of the schemes is set out in the study mentioned in footnote 5.

There are a number of ways in which EU citizenship or residence schemes can be abused for tax purposes. Individuals can declare residency in one of these jurisdictions yet their real tax residency may be in another jurisdiction (dual residency abuse). Under exchange of information agreements between jurisdictions information for tax purposes could be sent to the wrong jurisdiction of residence. With regard to tax avoidance, the management of business structures could be set up in EU citizenship or residence schemes jurisdictions that have low residence requirements not compliant with international rules to counteract tax avoidance, for example do not require substantive business activities, and/or where the business structure can take advantage of tax regimes which facilitate aggressive tax planning.

Additionally, competition among Member States for clients wishing to acquire citizenship or residence through investment schemes risks triggering a 'race to the bottom' over standards of due diligence and transparency.

Terrorist financing

The assessment of the terrorist financing threat related to golden visas/passports has identified the following areas of concern:

- **Security checks**: There are certain security obligations under EU law that must be carried out before issuing a visa or residence permit to foreign investors. However, there is a lack of available information on practical implementation and discretion in the way that Member States approach security concerns.

- **Physical residence requirement:** Residence permits obtained by investment, with limited or no required physical presence of the investor in the Member State in question, could have an impact on the application of EU long-term residence status and the rights associated with it, and may even provide a fast track to national and thus EU citizenship.

- **Lack of transparency:** The report stresses a lack of transparency and oversight of the schemes, in particular in terms of monitoring and the absence of statistics on how many people obtain a residence permit through such schemes.

Conclusions: Within the described context, the level of the terrorist financing threat related to golden visas/passports is considered as significant/very significant (level 3/4).

Money laundering

Examples of jurisdictions that have attracted wealthy people involved in money laundering schemes:

In recent years, Cyprus has become a financial refuge for Ukrainian and Russian oligarchs and a hub for money laundering operations. This is in part due to its streamlined CIP: wealthy foreigners can become citizens in less than 6 months in exchange for investing €2 million. Almost half of the 2,000 passports issued by the scheme in the last 2 years have been acquired by Russians. Such an investment may

legitimise laundered funds, and Cypriot citizenship may facilitate the transfer of money into the country and around the European financial market. Cyprus is also popular as it is a tax incentive country.

Maltese citizenship is similarly popular with wealthy Russians. Saudi Arabians have also invested in the scheme: for example, Waleed al-Ibrahim, chairman of the Middle East Broadcasting Center. Al-Ibrahim was arrested in November 2017 as part of a corruption purge.[147]

Caribbean Island passports are also implicated in enabling money laundering. An individual linked to the Azerbaijani Laundromat scandal was a Pakistani national, who also held St Kitts and Nevis citizenship; it is likely that the purpose of this citizenship was to hide assets.

Golden visas are also used to evade sanctions

Since the imposition of EU and U.S. economic sanctions, visa bans and asset freezes on Russia following its invasion of Ukraine and illegal annexation of Crimea in 2014, there has been a surge in Russian applications for CIPs; this has given rise to the risk of sanctions evasion in addition to the potential laundering of illicit funds.

North Korean nationals have also previously managed to obtain alternative passports, which they then used to conduct business based outside of North Korea – two North Koreans were identified using Kiribati and Seychelles passports to operate in Hong Kong and Japan. Whilst both nations have purportedly cancelled the scheme, it is believed that their passports were issued after the alleged cancellation date.

Lastly, the Comoros Islands CIP has received negative press: in early January 2018, the government of Comoros cancelled 170 passports allegedly improperly issued to foreigners, including many Iranians, during the tenure of the previous government. The Comoros authorities have found that at least two foreign holders of Comoros passports are alleged by US authorities to have violated sanctions against Iran (although in neither instance does Comoros citizenship itself appear to have directly influenced the evasion).

Thus, the primary risk of these schemes is that of **exposure to money laundering.** There is a clear and definite risk that certain clients may have been given lower risk ratings (as determined by their nationality) than is warranted. This could affect the level of client due diligence performed and/or transaction monitoring applied. It may result in the clearance of transactions that, while apparently benign, should have undergone greater scrutiny due to underlying circumstances.

---

[147] See, in general: www.transparency.org/whatwedo/publication/golden_visas
Also:
https://www.maltatoday.com.mt/news/national/83539/russian_nationals_dominate_list_of_global_rich_who_are_now_maltese#.XSxUtCBS-Uk
http://www.independent.com.mt/articles/2018-12-30/local-news/Turkish-billionaires-and-Russian-industry-moguls-meet-Malta-s-new-citizens-6736201441

Conclusions: In the light of the scenario described above, the level of the money laundering threat related to golden visas/passports is considered as significant/very significant (level 3/4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to golden visas/passports has identified the following areas of concern:

a) risk exposure

The two main areas of concern assessed by the European institutions are those of security and transparency and information. On security, it has been found that checks run on applicants are not sufficiently robust and that the EU's own centralised information systems, such as the Schengen Information System, are not being used as systematically as they should be. On transparency and information, there is a lack of clear information on how the schemes are run, including on the number of applications received, granted or rejected and the origins of the applicants. In addition, Member States do not exchange information on applicants for such schemes, nor do they inform each other of rejected applicants.

b) risk awareness

National authorities involved do not seem to be aware of the problems involved in these schemes or, in the worst case scenarios, willingly assume the schemes' inherent risks in exchange for expected investments.[148]

Recent scandals reported in the media suggest that some EU countries have not made it standard procedure to carry out enhanced checks on applicants, their family members and the origin of their funds.

c) legal framework and controls

Security checks: There are certain security obligations under EU law that must be carried out before issuing a visa or residence permit to foreign investors. However, there is a lack of available information on practical implementation and discretion in the way that Member States approach security concerns.

Physical residence requirement: Residence permits obtained by investment, with limited or no required physical presence of the investor in the Member State in question, could have an impact on the application of the EU long-term residence status and rights associated with it, and may even provide a fast track to national and thus EU citizenship.

[148] IMF Working Paper, WP/15/93, Too Much of a Good Thing?: Prudent Management of Inflows under Economic Citizenship Programs, by Xin Xu, Ahmed El-Ashram and Judith Gold https://www.imf.org/external/pubs/ft/wp/2015/wp1593.pdf

Conclusions: In this context, the level of terrorist financing vulnerability related to golden visas/passports is considered as significant/very significant (level 3/4).

Money laundering

The assessment of money laundering vulnerability relies on the same inherent factors described above and is not treated separately. Nevertheless, specific consideration of its high vulnerability is necessary, in light of the high levels of corruption, tax evasion, criminal activities and money laundering cases detected and treated by law enforcement authorities.

Conclusions: In this context, the level of money laundering vulnerability related to golden visas/passports is considered as very significant (level 4).

Mitigating measures

The schemes described are of common EU interest since every person that acquires the nationality of one Member State will simultaneously acquire **EU citizenship.** The decision by one Member State to grant citizenship in return for investment automatically gives rights in relation to other Member States, in particular rights of free movement and access to the EU internal market to exercise economic activities, as well as the right to vote and be elected in European and local elections. In practice, these schemes are often advertised as a means of acquiring EU citizenship, together with all the rights and privileges associated with it.

Apart from the basic ethical considerations about the selling of citizenship and the unsettling notion that some Member States are profiting from the sale of a shared European asset, there is a distinct and inherent series of risks connected with these schemes.

For the Commission:

The Commission will **monitor wider issues of compliance with EU law** raised by investor citizenship and residence schemes and will take necessary action as appropriate. For this reason, Member States need to ensure in particular that:

- all obligatory border and security checks are systematically carried out;
- the requirements of the Long-Term Residence Permit Directive and the Family Reunification Directive are properly complied with;
- funds paid by investor citizenship and residence applicants are assessed according to the **EU anti-money laundering rules**;

- **Directive 2018/822/EU**[149] which requires intermediaries to submit information on reportable cross-border tax arrangements to their national authorities[150] comes into effect as from 2020;
- the Commission intends to monitor steps taken by Member States to address issues of transparency and governance in managing these schemes. It established a **group of experts from Member States** to improve the transparency, governance and security of the schemes. That group is tasked in particular with:
  - setting up a system of exchange of information and consultation on the numbers of applications received, countries of origin and the number of citizenships and residence permits granted/rejected by Member States to individuals based on investments;
  - developing a common set of security checks for investor citizenship schemes, including specific risk management processes, by the end of 2019.

Finally, concerning third countries setting up similar schemes, which may have security implications for the EU, the Commission intends to monitor investor citizenship schemes in candidate countries and potential candidates as part of the EU accession process. It will also monitor the impact of such schemes by EU visa-free countries as part of the visa-suspension mechanism.

For the Member States:

Member States should ensure transparency and good governance in the implementation of the schemes, with a view to addressing in particular risks of infiltration of the EU economy by non-EU organised crime groups, as well as risks of money laundering, corruption and tax evasion. Action by Member States should include:

- annual reporting exercises that are made publicly available;
- making sure that the reports include data on the numbers of received applications, countries of origin and the number of citizenships and residence permits granted and rejected – alongside the identity and country of origin of the newly accepted residents and citizens;
- providing disaggregated statistics on investor residence schemes, so that the specific ground for residence or the investment option chosen can be identified;
- putting in place a risk management process, including an appropriate identification, classification and mitigation of risks, under the coordination of a national designated authority. Monitor the implementation of the plan;
- carrying out an annual audit exercises to assess the implementation of the risk management plan;

[149] Council Directive (EU) 2018/822 of 25 May 2018 amending Directive 2011/16/EU as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements; OJ L 139, 5.6.2018, p. 1-13.
[150] Administrative cooperation in (direct) taxation in the EU: https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en.

· in the context of **tax avoidance and tax evasion risks**, there are tools available in the EU framework for administrative cooperation (Directive 2011/16/EU[151]), in particular the spontaneous exchange of information. which will allow, for example, the competent authorities of the citizenship/investor residence scheme Member State to inform the Member State of residence of the individual obtaining the benefit of such a scheme.

Member States should also clarify and publicise criteria for assessing applications and security checks performed as part of the scheme, and ensure regular *ex post* monitoring of compliance with these criteria, in particular with regard to the investment made by the applicant. They should also introduce a procedure for revoking the permits should criteria be no longer fulfilled.

Last but not least, Member States should also offer total transparency on the processes followed to award the management of these schemes to private companies, up to and including information on such companies' beneficiary ownership. Under no circumstances should these private companies be involved in the actual verification of the information and documents provided by the applicants: these checks should remain in the hands of the responsible government bodies, rather than with private entities.

ANNEX 2 – EU LEGAL FRAMEWORK ON ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING

EU legislation on financial services and supervision which is relevant for the AML/CFT field based on Article 53 and Article 114 TFEU:

- Directive (EU) 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
- Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.
- Directive 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
- Directive 2013/36/EU 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 TFEU and Article 33 relating to controls of cash movements at the external border of the EU:

[151] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

- Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (the new Cash Control Regulation).

Additional preventative measures:

- Directive (EU) 2018/1673 on combating money laundering by criminal law.
- Regulation (EU) 2019/880 on the introduction and the import of cultural goods.[152]

Other areas relevant to AML/CFT are covered by EU legislation adopted in the CFT field based on article 215 TFEU and article 75 TFEU and 352 TFEU – imposing targeted financial sanctions:

- Council Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism.
- Council Regulation (EC) No 881/2002 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 concerning restrictive measures against Iran and repealing Regulation (EU) No 961/2010.

EU legislation adopted in the AML/CFT field based on TFEU provisions in the area of freedom, security and justice

- Council Decision 2000/642/JHA concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information.
- Council Decision 2007/845/JHA 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 2001/500/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime.
- Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA.
- Council Framework Decision 2005/212/JHA on confiscation of crime-related proceeds, instrumentalities and property.
- Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence.

[152] Regulation (EU) 2019/880 of the European Parliament and of the Council of 17 April 2019 on the introduction and the import of cultural goods; PE/82/2018/REV/1; OJ L 151, 7.6.2019, p. 1–14. .

- Council Framework Decision 2006/783/JHA on the application of the principle of mutual recognition to confiscation orders.
- Directive 2014/41/EU regarding the European Investigation Order in criminal matters.
- Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

ANNEX 3 – GLOSSARY

Anti-money laundering related acronyms and abbreviations	
Acronym	**Meaning**
ACH	Automated Clearing House
AML/CFT	Anti-Money Laundering / Counter-Terrorism Financing
AMLID	Anti-Money Laundering International Database
APG	Asia/Pacific Group on Money Laundering
API	Authorised Payment Institutions
APTs	Asset Protection Trusts
ARS	Alternative Remittance System
ATM	Automated Teller Machine
BO	Beneficial Owner
BSA	Bank Secrecy Act
CCR	Cash Control Regulation
CCTV	Closed-Circuit Television
CDD	Customer Due Diligence
CIP	Customer Identification Program
CTR	Currency Transaction Report
DNFBPs	Designated Non-Financial Businesses and Professions
EAG	Eurasian Group on Combating Money Laundering and Financing of Terrorism
EBA	European Banking Authority http://www.eba.europa.eu/
ECB	European Central Bank
ECEF	Electronic Continuing Examination Folder
EDD	Enhanced Due Diligence
EFT	Electronic Funds Transfer

EGMLTF	Expert group on Money Laundering and Terrorist Financing (E02914)
Egmont Group	the Egmont Group of Financial Intelligence Units (informal international network of FIUs)
EIOPA	European Insurance and Occupational Pensions Authority https://eiopa.europa.eu/
ESAs	The three European Supervisory Authorities (EBA, EIOPA and ESMA)
ESAAMLG	Eastern and Southern African Anti-Money Laundering Group
ESMA	European Securities and Markets Authority https://www.esma.europa.eu/
FATF	Financial Action Task Force www.fatf-gafi.org FATF was chartered in 1989 by the Group of Seven industrial nations to foster the establishment of national and global measures to combat money laundering. It is an international policy-making body that sets anti-money laundering standards and counter-terrorist financing measures worldwide. Its Recommendations do not have the force of law. Thirty-five countries and two international organizations are members. In 2012, FATF substantially revised its 40 + 9 Recommendations and reduced them to 40. http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods.
FI	Financial Institution
FinCEN	Financial Crimes Enforcement Network
FinTech	Technology-enabled and technology-supported financial services
FIU	Financial Intelligence Units
FSRB	Financial Action Task Force-Style Regional Body
FTF	Foreign Terrorist Fighters
GAFILAT	Financial Action Task Force on Money Laundering in Latin America

GDP	Gross Domestic Product
IA	Impact Assessment
IBC	International Business Company
IVTS	Informal Value Transfer System
KYC	Know Your Customer
KYE	Know Your Employee
LEA	Law enforcement authority
MER	Mutual Evaluation Report
ML	Money laundering
MENAFATF	Middle East and North Africa Financial Action Task Force
MLAT	Mutual Legal Assistance Treaty
MLRO	Money Laundering Reporting Officer
MONEYVAL	Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures https://www.coe.int/en/web/moneyval Formerly PC- R-EV, the committee was established in 1997 by the Committee of Ministers of the Council of Europe to conduct self and mutual assessments of anti-money laundering measures in place in Council of Europe countries that are not FATF members. MONEYVAL is a sub-committee of the European Committee on Crime Problems of the Council of Europe (CDPC).
MOU	Memorandum of understanding
MSB	Money Services Business
MVTS	Money Value Transfer Services
NPO	Non-for-profit organisations
NRA	National risk assessment
OCG	Organised Crime Group
OECD	Organization for Economic Cooperation and Development http://www.oecd.org/

	International organization that assists governments on economic development issues in the global economy. OECD houses the FATF secretariat in Paris.
OFC	Offshore Financial Center
PEP	Politically Exposed Person
PIC	Private Investment Company
PSD	Payment Services Directive
RBA	Risk Based Approach
ROE	Report of Examination
SAR	Suspicious Activity Report
SNRA	Supra-national risk assessment
SPSP	Small Payment Services Provider
STR	Suspicious transactions reports
TBML	Trade-Based Money Laundering
TCSPs	Trust and Company Service Providers
TF	Terrorist financing
TI	Transparency International https://www.transparency.org/ Berlin-based, non-governmental organization dedicated to increasing government accountability and curbing both international and national corruption. Established in 1993, TI is active in approximately 100 countries. It publishes "corruption news" on its website daily and offers an archive of corruption- related news articles and reports. Its Corruption Online Research and Information System, or CORIS, is perhaps the most comprehensive worldwide database on corruption. TI is best known for its annual Corruption Perceptions Index (CPI), which ranks countries by perceived levels of corruption among public officials; its Bribe Payers Index (BPI) ranks the leading exporting countries according to their propensity to bribe. TI's annual Global Corruption Report combines the CPI and the BPI and ranks each country by its overall level of corruption. The lists help financial institutions determine the risk associated with a particular jurisdiction.
UBO	Ultimate Beneficial Owner

UCITS	Undertakings for Collective Investment in Transferable Securities
UTR	Unusual Transaction Report

ANNEX 4 – BIBLIOGRAPHY

1/ Commission documents

February 2016 – Communication from the Commission to the European Parliament and the Council on an Action Plan for strengthening the fight against terrorist financing.
https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52016DC0050

March 2016 — Commission Staff Working Document on the movement of capital and the freedom of payment (SWD(2016) 105).
https://ec.europa.eu/.../documents/2019-capital-market-monitoring-analysis_en.pdf

July 2016 — Impact assessment accompanying the Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.
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

January 2017 - Strengthening Citizens' Rights in a Union of Democratic Change EU. Citizenship Report 2017
https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017DC0030

June 2017 – Commission staff working document on improving cooperation between EU Financial Intelligence units
https://ec.europa.eu/newsroom/document.cfm?doc_id=45318

December 2017 – Identifying market and regulatory obstacles to crossborder development of crowdfunding in the EU
https://ec.europa.eu/info/publications/171216-crowdfunding-regulatory-obstacles-crossborder-development_en

March 2018 – Commission proposal for a regulation on European crowdfunding services providers.
https://ec.europa.eu/info/publications/180308-proposal-crowdfunding_en

March 2018 - FinTech Action plan: For a more competitive and innovative European financial sector.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109

January 2019 - Investor Citizenship and Residence Schemes in the European Union.
https://ec.europa.eu/info/sites/info/files/com_2019_12_final_report.pdf

March 2019 - Communication from the Commission to the European Parliament, the European Council, the Council and the European Central Bank Deepening Europe's Economic Monetary Union: Taking stock four years after the Five Presidents' Report.
https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20190306_com-2019-126-report_en.pdf

2/ European Parliament documents

2018 – EP / ECON Committee: The supervisory approach to anti-money laundering: an analysis of the Joint Working Group's reflection paper
http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/624424/IPOL_IDA(2018)624424_EN.pdf

2018 – EP / ECON Committee: Money laundering - Recent cases from a EU banking supervisory perspective
http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2018)614496

2018 – EP / ECON Committee: Virtual Currencies. Monetary Dialogue July 2018
http://www.europarl.europa.eu/cmsdata/149902/KIEL_FINAL%20publication.pdf

2018 – EP / ECON Committee: Virtual Currencies in the Eurosystem: challenges ahead. Monetary Dialogue July 2018
http://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf

2018 – EP / TERR Committee: Virtual currencies and terrorist financing: assessing the risks and evaluating responses
http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf

2018 - Citizenship and residency by investment schemes in the EU: State of play, issues and impacts
www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2018)627128

3/ Eurostat reports

Personal remittances statistics, Statistics explained, Eurostat - 2017.
http://ec.europa.eu/eurostat/statistics-explained/index.php/Personal_remittances_statistics

Handbook on the compilation of statistics on illegal economic activities in national accounts and balance of payments – 2018 edition.
https://ec.europa.eu/eurostat/documents/3859598/8714610/KS-05-17-202-EN-N.pdf/eaf638df-17dc-47a1-9ab7-fe68476100ec

4/ Europol reports

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

Europol Financial Intelligence Group, Report '*From suspicion to action'*, 2017.
https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact

5/ Other Union-level bodies

ECB payment statistics reports.

ECB 2014 Working paper on consumer cash usage.
https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf

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

2017 - European Supervisory Authorities' Joint Guidelines, the Risk-Based Supervision Guidelines.
https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20%28ESAs%202016%2072%29.pdf

2019 – EBA Report with advice for the European Commission on crypto-assets
https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

2019 – ESMA Advise to the European Union Institutions on Initial Coin Offering and Crypto-Assets
https://www.esma.europa.eu/press-news/esma-news/crypto-assets-need-common-eu-wide-approach-ensure-investor-protection

6/ 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

2018 – Financing of Recruitment for Terrorist Purposes
http://www.fatf-gafi.org/publications/methodsandtrends/documents/financing-recruitment-terrorist-purposes.html

2018 – G20 commitment to implement FATF standards and support for work on crypto assets.
http://www.fatf-gafi.org/media/fatf/documents/reports/FATF-Report-G20-FM-CBG-July-2018.pdf

2018 – Moneyval's Annual report for 2017
https://rm.coe.int/moneyval-annual-report-2017-eng/16808af3c2

2019 – Risk-based Approach for Trust and Company Service Providers
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-trust-company-service-providers.html

2019 – Guidance for a Risk-based Approach for the Accounting Profession
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-accounting-profession.html

2019 – Risk-based Approach for Legal Professionals
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-legal-professionals.html

2019 – Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.
http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

7/ Other external information sources

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

Transparency International/Global Witness, European Getaway 2018 – Inside the Murky World of Golden Visas.
www.transparency.org/whatwedo/publication/golden_visas

8/ Confidential information

Information was received from Europol (classified).

9/ Oral and written contributions from the following stakeholders

The Commission consulted the Member States by means of a questionnaire in July 2018, with enclosures on:

- national mitigating measures;
- templates for financial and prosecution ML/TF data; and
- emerging risks.

By the end of 2018, the Commission had received 23 replies. Subsequently, Member States were further consulted in dedicated meetings of the Expert Group on Money Laundering and Terrorist Financing on 10 December 2018 and 11 February 2019.

In November-December 2018, the Commission held four workshops with private-sector stakeholders, one with representatives of financial institutions, two with 'designated non-financial businesses and professions' (DNFBPs), and one with civil society (NPOs) and academics. A second phase of this round of meetings took place in January 2019. The oral input from the private sector was complemented by 15 written replies.

National associations were represented through their respective European federation:

- Accountancy Europe
- Antwerp World Diamond Centre private foundation
- 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
- Electronic Money Association
- 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 Federation of Building Societies
- European Federation of Jewellery (EFJ)

- European Foundations Centre
- European Fundraising Association (EFA)
- 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
- NGO Voice
- Open Society Foundation
- PayPal
- Remote Gambling Association
- STEP
- SWIFT
- Università Catolica del Sacro Cuore
- Taxadvisers Europe
- Transparency International EU
- The Association for Financial Markets in Europe (AFME)
- The Council of Bars and Law Societies of Europe
- Trust Europe Affairs (virtual currencies)
- Voice
- Visa
- Western Union Europe.