EUROPEAN
COMMISSION

Brussels, 27.10.2022
SWD(2022) 344 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(2022) 554 final}

Table of Contents

1. INTRODUCTION

This Supra-National Risk Assessment (SNRA) follows the methodology[1] used for the 2017 and 2019 SNRAs, which provides a systematic analysis of the money laundering and terrorist financing risks linked to the methods used by perpetrators. The aim is to identify circumstances in which services and products in a given sector could be abused for money laundering (ML) or terrorist financing (TF) purposes, without passing judgement on the sector as a whole.

As with its previous editions, 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 Directive 2015/849 ('the 4th Anti-Money Laundering Directive') as modified by Directive 2018/843 ('the 5th Anti-Money Laundering Directive'), hereby 'the Anti-Money Laundering Directive' or 'the AMLD', if Member States decide not to apply any of the previous SNRA recommendations, they should notify the Commission of their decision and provide a justification for it ('comply or explain'). No such notification was received to date by the Commission.

Process followed for the 3rd edition of the Commission SNRA

The Commission has built this third edition of the SNRA updating the analysis and conclusions of its second edition as well as further consulting individual experts, private stakeholders (representative organizations at EU level) and national authorities. These consultations have taken place from 2020 to 2022.

The Commission also consulted other regulatory agencies and national authorities, such as Europol, the European supervisory authorities (ESAs) and the FIUs' Platform (FIUnet)[2].

The purpose of this consultation exercise was twofold: to follow up on the recommendations made in the 2019 SNRA and to update and further fine-tune its analysis and conclusions, mainly as regards quantitative data and perceived risk levels.

Finally, given the evolving nature of ML/TF threats and vulnerabilities, the SNRA takes 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 assessment takes due account of national risk assessments (NRAs) produced by the Member States to ensure the proper identification and mitigation of specific national risks[3].

Individual sectors are also assessed taking stock of their relevant risk factors, including those relating to specific customers, countries, products, services, transactions and delivery channels.

[1] A detailed description of the methodology followed appears in **Annex 2.**
[2] The network of Financial Intelligence Units (FIUs).
[3] For this exercise the Commission has to date received the most recent NRA from all Member States (as well as from Iceland, and Norway) except Portugal and Romania.

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.

During this exercise Commission analysis has also benefited from the audit conducted by the European Court of Auditors (ECA) during 2019-2020. This audit has led to the adoption by the ECA of a special report[4].

The conclusions of the ECA report as well as the methodology followed by the Commission in its SNRAs are further discussed under **Annex 2** ("Methodology").

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 the 4th Anti-money Laundering Directive as modified by the 5th Anti-Money Laundering Directive. Transposition deadline for the latter elapsed on January 20, 2020. At the time of drafting this report, all Member States save the Netherlands have declared a complete transposition.

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 3.**

In addition, an index of abbreviations used in the risk analysis is attached in **Annex 4** and a bibliography in **Annex 5.**

[4] ECA special report pursuant to Article 287(4), second subparagraph, TFEU: "Special Report 13/2021: EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient": https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=58815

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). **Methodology is presented in detail in Annex 2.**

It is based on Directive (EU) 2015/849 (4th Anti-money Laundering Directive) as modified by Directive (EU) 2018/843 (the AMLD).

Each risk is rated for threat and vulnerability. The ratings are on a scale from 1 to 4 and coloured for easy identification 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.

The final (or *residual*) risk level is ultimately determined by combination between the threat versus vulnerability. The risk matrix determining this risk level is based on a weighting of 40% (threat) + 60% (vulnerability) – assuming that the vulnerability component has more capacity in determining the risk level.

The risk matrix:

Threat					
	Very significant	2,2	2,8	3,4	4
	Significant	1,8	2,4	3	3,6
	Moderately significant	1,4	2	2,6	3,2
	Lowly significant	1	1,6	2,2	2,8
		Lowly significant	Moderately significant	Significant	Very significant
		Vulnerability			

Then, the residual risk level is presented for every product/sector in a graded table:

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

CASH-RELATED PRODUCTS

1. Cash couriers

Product

Cash couriers / cross external border cash movements

Sector

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

Since 15 June 2007, movements of cash entering or leaving the EU had been governed by Regulation 1889/2005, which implements Recommendation 32 of FATF on cash couriers at EU level. That Regulation is an integral part of the EU's Anti-Money Laundering and Terrorist Financing framework. 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 Cash Controls Regulation in December 2016. Regulation (EU) 2018/1672[5] was adopted in October 2018 and has entered into application on 3rd June 2021 (the new Cash Controls Regulation).

Regulation 1889/2005 established a uniform EU approach towards cash controls based on a mandatory declaration system. If a natural person entering or leaving the EU (including transiting) with cash of a value of EUR 10 000 or more, they should declare them to the relevant customs authorities. 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 were indications of illegal activities linked with movements of cash lower than EUR 10 000, the collecting and recording of information related to these movements was 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).

In keeping with the latest developments in international standards on combating money laundering and terrorism financing developed by the FATF, the new Cash Controls Regulation has significantly beefed up controls both in terms of scope and in terms of authorities' powers:

- In terms of scope, under the new Cash Controls Regulation, the definition of cash has been extended to cover not only currency and bearer negotiable instruments (e.g. cheques or money orders) but also commodities used as highly-liquid stores of value such as gold. Its scope was also extended to cover cash that is sent by post, freight or courier shipment;
- The new Cash Controls Regulation also provides for the obligation for 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 is required irrespective of whether travellers are carrying the cash in person, in their luggage or means of transport and the cash has to be made available for control;
- Moreover, where the cash is sent by other means ("unaccompanied cash"), the relevant authorities have the power to ask the sender or the recipient to make a disclosure declaration. The authorities are able to carry out controls on any consignments, packages or means of transport which may contain unaccompanied cash.
- The new Cash Controls Regulation enables Customs authorities to act on amounts lower than the threshold of EUR 10 000, where there are indications that cash is related to criminal activity.

In addition, the Regulation further enhances coordination of actions across authorities:

[5] Regulation No 1889/2005/EC, *OJ L 284, 12.11.2018, p. 6–2.*

- The new Regulation improves the exchange of information between authorities (Customs and Financial Intelligence Units) and Member States[6].
- In case where there are indications that cash is related to criminal activity which could adversely affect the financial interests of the EU, this information is also transmitted to the European Commission, the European Public Prosecutor's Office and to Europol, where they are competent to act;
- The new Cash Controls Regulation provides in its Article 5(4) that the risk assessments produced by the Commission and by national Financial Intelligence Units (FIUs) will be taken into account when establishing the common risk management framework for performing controls.

The new Cash Controls Regulation does 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 fundamental freedoms.

Before the pandemic, per year on average there were around 110 000 cash cases, representing a total amount of around EUR 55 billion. Customs controls detected around 13 000 cases where cash was not declared or was incorrectly declared representing around EUR 364 million per year.

As of the second quarter of 2020, due to the pandemic, travel was severely disrupted and, consequently also the physical movement of cash resulting to lower values of cash controls declarations (and non-declared cash or incorrect declarations) than the previous years.

For 2020, there were almost 57 000 cash cases, representing a total amount of around EUR 37 billion. Customs controls detected almost 9 000 cases where cash was not declared or was incorrectly declared representing around EUR 245 million.

Description of the risk scenario

This risk scenario is intrinsically linked to use of/payment in cash and to high value denomination banknotes risk scenario[7].

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 access to placement in the legal economy is easier. This includes locations characterised by a predominant use of cash, more lax supervision of the financial system or stronger bank secrecy regulations. Terrorists may also 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. To move very large amounts of cash, perpetrators often 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 (except cargo) 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.

[6] Deadline of 15 days for data to be submitted to national FIU (declarations and infringements) and 15 days for infringements being shared with all MS customs administrations.
[7] 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

On the other hand, the seizure of large amounts of cash within EU is also possible. It is not only important to control EU external borders, but also the intra-EU transportation of cash. This fact is relevant because of the different intra-EU rules that Member States have regarding the use of cash to, for instance, purchase goods, deposit in bank accounts, etc. Additionally, the external borders are not monitored with the same efficiency level. Criminals know that fact, and they try to cross the most permeable borders with cash, even if they have to drive thousands of kilometres within EU. National thresholds of intra-EU movements of cash exist in some Member States: in Spain, for instance, it is EUR 100 000 for internal travel and EUR 10 000 when crossing borders.

Example: Cash generated by criminal activities laundered by the purchase of high value goods and properties (Europol Report "*Why is cash still king*")

Money from the sale of drugs was collected in Member State 1 and its laundering was orchestrated through the movement of cash by couriers acting as mules from Member States 1 to Member States 2, where cash was used to buy gold. Thereafter, gold was transported to and made into jewellery in a third country. A key organiser admitted laundering EUR 36 million since 2010 and sending 200 kg of gold from EU to the third country. The network collected about EUR 170 million per year.

A cash payment threshold in Member State 2 would have reduced the profitability of this criminal scheme (as intermediaries have to be paid and multiplying transactions to change cash into gold by non-professional would have aroused more suspicion).

Threat

Terrorist financing

Terrorist groups have made use of various techniques to move physical cash across the external borders, particularly in the case of larger organisations. This includes the following:

- The threat is particularly relevant for cash couriers from the EU to third countries. Law enforcement authorities have seized large amounts of money in conflicts zones that was supposed to finance terrorist organisations;
- Cases have been identified where (prospective) foreign terrorist fighters doubled as cash couriers to fund their travels and sojourn in conflict areas. These individuals typically carry lower amounts that are more difficult to detect and may not be subject to an obligation to declare incumbent on natural persons carrying EUR 10 000 Euro or more is cash. As it allows for anonymity, this modus operandi is perceived as attractive and fairly secure, despite still carrying some risks. That is the reason why this modus operandi shall also be considered in conjunction with the analysis of high denomination banknotes. The more high denomination banknotes are used, the easier the cash transportation is – although risks associated with acquiring high denomination notes (not readily available) may not outweigh the benefit of additional compactness. Cash transportation 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 (e.g. prepaid cards)[8].

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

Threats posed by cash couriers have been documented in the FATF Report: Money laundering through the physical transportation of cash (October 2015)[9].

That report points to physical transportation of cash across an international border, as 'one of the oldest and most basic forms of money laundering'. Transportation of cash is also used for terrorist financing[10]. 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 explains 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 highlights that criminals exploit the existing cash declaration systems mechanisms, for example, by 'reusing cash declarations several times for the same purpose'[11].

In the above-mentioned 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 have revealed 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 access to placement in the legal economy is easier (in particular 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 criminals 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 regard to money laundering. European investigations indicate that movements of cash inside the EU and outside are associated with criminal offences. The

[8] For prepaid cards, under the New Cash Controls Regulation, 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.
[9] http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf
[10] FATF report. p. 3.
[11] Ibid., p. 16

most relevant crime area is drug trafficking[12]. Drug related cash proceeds generated through the sales and distribution of predominantly cocaine and hashish are accumulated and received by the designated collectors working for a money laundering controller network. The money laundering controller networks provide money laundering as a service -cash out, cash in and payment for third parties- to any criminal organisation that approaches them. They offer similar services than financial institutions do, but outside of the regulated financial framework.

The drug trafficking organizations (DTO) then engage with money laundering controller networks(traditionally outside of the EU)these controllers charge a commission for facilitating towards the DTOs the value of their proceeds. The money laundering controller networks dispose of their own cash pool in different countries operated by coordinators and cash collectors. 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 (still within the EU) or exiting directly the EU. The current legal framework 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[13] or is transported out of the EU towards "cash friendlier" jurisdictions. Turkey, Dubai and Beirut have in the last years shown steady presence as preferred cash destinations and growing financial hubs in the EU.

The use of cash, sometimes in conjunction with other tools such as trade-based transactions, crypto currencies and hawala, is also an essential part of the drug trade, all the way from street level to purchase in production countries.

Europol Financial Intelligence Public Private Partnership (EFIPPP) information extracted from typologies:

Traffic of human beings: Organised crime groups involved in this traffic send cash/invest illegal profits in the country of origin: using cash couriers and Money Service Businesses (MSBs)(Western Union, MoneyGram) and / or invest in real estate, luxury vehicles and cash intensive businesses. In case of use of cash couriers: difficulty in financial detection.

Illegal trade: Related to drugs, organised networks of 'collectors' physically gather and transport criminal proceeds in the form of cash, precious metals and jewellery.

Match-fixing/betting: a ML indicator is the widespread use of cash couriers, MSBs and increasingly e-wallets payment service providers to transfer the proceeds of crime linked to sports corruption cases and to fuel online betting accounts for large-scale match-fixing operations.

ML Controller Networks: the movement of value by cash couriers is one of the techniques mentioned. Cash carriers collect the ill-gotten funds –usually cash- to be transported to the required destination.

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

Vulnerability

Terrorist financing

[12] Europol, Operation Jumita, carried out by Spanish Authorities, 10 June 2021:1,6 tonnes of cocaine and EUR 16,5 million confiscated in largest cash seizure from a criminal organisation in EU.

[13] 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.

a) Risk exposure

The cash couriers are associated with the threat of the large denomination banknotes: 500 (no longer issued since April 2019) and 200 Euro. 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 Cash Control Regulation – but is more limited.

c) Legal framework and checks

There are controls in place through the mandatory declaration of cash transportation at the EU external borders[14]. Under the new Cash Controls Regulation these controls are extended to cash sent in postal parcels or freight shipments, and to commodities used as highly- liquid stores of value such as gold, which were not previously subject to cash controls. This legislation has also increased the risk awareness.

Where unaccompanied cash is concerned (cash sent through consignments or parcels) the new Cash Controls Regulation enables the competent authorities to request the sender or the recipient, as the case may be, to make a disclosure declaration The authorities will also have the power to carry out controls on any consignments, receptacles or means of transport which may contain unaccompanied cash.. The declarations and disclosure declarations are done in writing or electronically using a standard form. These cash declarations allow for more effective reporting to the FIUs.

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

[14] Intra-EU controls for intra-EU transportation of cash also exists in a number of Member States but these controls and rules are not harmonised across the EU (in particular in terms of thresholds). See reference in Payment in cash fiche to its Report "Why is cash still a king?": "… *many EU Member States have no provisions to control cash movements within the EU territory, and there is significant variation in the regulatory framework for those which do. As such, once criminal cash has entered the EU, certain routes and intra-EU borders may be vulnerable to criminals who will select them due to absence of any risk of controls. Consideration should be given to a more harmonised approach among EU MS concerning cash movements within the EU."*
https://www.europol.europa.eu/publications-events/publications/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering#downloads

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 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 checks

Similarly to TF, there are controls in place through the mandatory declaration of cash transportation at the EU external borders (Cash Controls 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 shipments deemed 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.

Conclusion: 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as very significant (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant/very significant (level 4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, terrorist financing and money laundering is VERY HIGH.

Mitigating measures

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

- It enables authorities to act on amounts lower than the declaration threshold of EUR 10 000, where there are indications that cash is related to 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 commodities used as highly-liquid stores of value such as gold.

For the Member States:

- Given the difficulties caused by non-harmonised intra-EU movements of cash rules, Member States could consider aligning those national thresholds.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol. In particular, relevant authorities in Member States should consider reporting to Europol the cash seizures and related information (destination/origin/type of banknotes…)[15].

[15] Within the limits of the applicable legal frameworks. Art. 10(2) of Regulation 2018/1672 provides for the transmission of the relevant information to Europol where it is competent to act under Article 3 of Regulation (EU) 2016/794, i.e.: only in case there are indications that cash is related to criminal activity which could adversely affect the financial interests of the Union.

2. Cash intensive business

Product

Cash intensive business

Sector

Cash intensive businesses include 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.

An insightful description of the use of cash features in European Central Bank's report "Trends and developments in the use of euro cash over the past ten years"[16] (published as part of the ECB Economic Bulletin, Issue 6/2018)[17]. In terms of transactions, 83% of the transactions in restaurants, bars and cafés and for hotels and accommodation were made using cash while this share was 48% in shops selling durable goods[18].

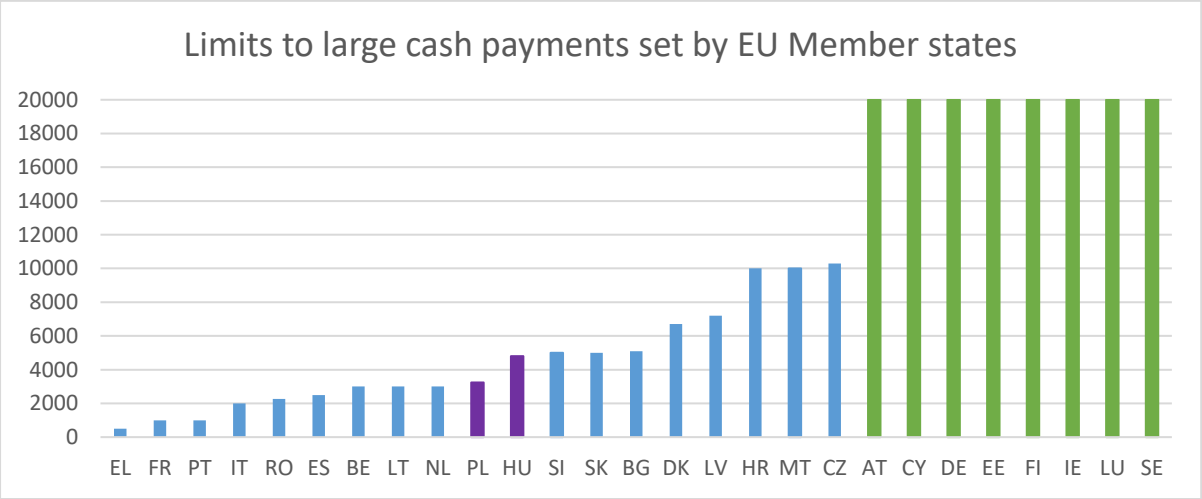
In order to increase vigilance and mitigate the risks posed by cash payments, the AML Directive subjects persons trading in goods to AML/CFT requirements when they make or receive cash payments of 10 000 EUR or more, including through linked payments. This measure does not amount to a blanket restriction on the use of cash, and its effectiveness heavily hinges on faithful adherence and implementation by private sector as well as effective oversight on part of national public authorities. Therefore, the Directive recognises that Member States may take different approaches, and allows them to lower the above threshold, introduce additional general limitations to the use of cash, or adopt other stricter measures.

Measures adopted at national level vary from one Member State to another:

- Currently, 19 Member States have introduced or are introducing limitations to cash payments19, ranging from EUR 500 in Greece to EUR 10 300 in the Czech Republic, with an average value of about EUR 4 500[20];
- The situation is constantly evolving, with Malta having recently introduced a limit of EUR 10 000 to payments in cash for some sectors, and other Member States having decided or planning to lower these limits (e.g. Denmark is planning to lower the limit to DKK 20 000 / EUR 2 700 and Italy will see its limit lowered to EUR 1 000 as of 2022);
- In three cases (France, Italy and Spain), higher thresholds apply to non-residents (between EUR 10 000 and EUR 15 000);
- In Hungary and Poland limits apply only to business-to-business (B2B) transactions, while some countries such as Slovenia have set different thresholds for business-to-consumers (B2C) and B2B transactions;
- Among the countries that have not set any limit to cash payments, Ireland and Sweden allow traders to refuse payments in cash.

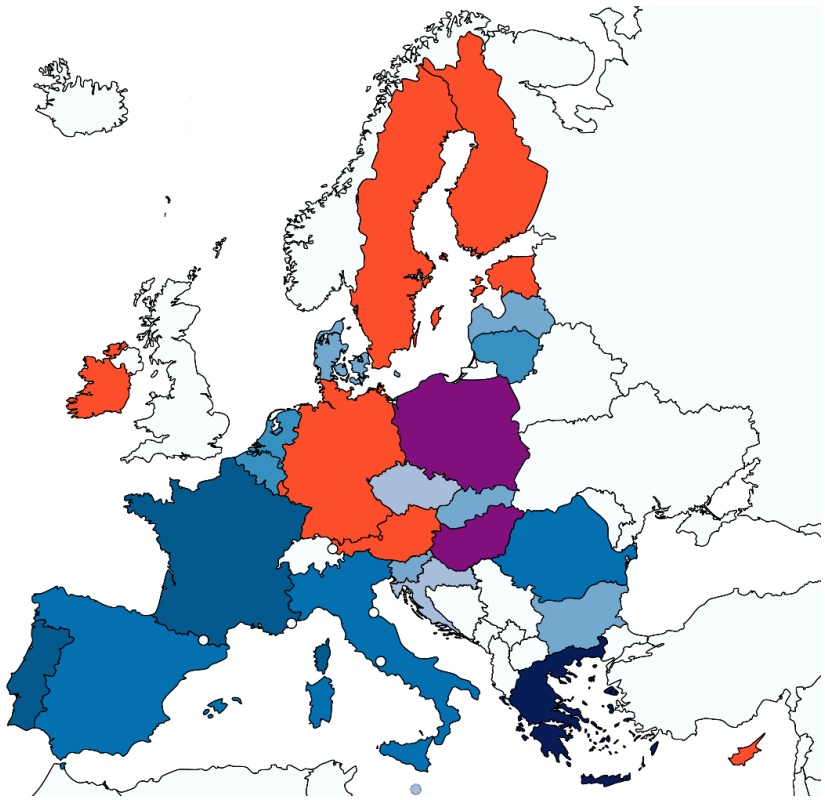
[16] https://www.ecb.europa.eu/pub/economic-bulletin/articles/2018/html/ecb.ebart201806_03.en.html
[17] https://www.ecb.europa.eu/pub/economic-bulletin/html/eb201806.en.html
[18] See ECB, December 2020, Study on the payment attitudes of consumers in the euro area (SPACE).
[19] In the case of the Netherlands, this is a draft proposal approved by the government on 25 September 2020.
[20] Figures refer to B2C transactions.

The graph below summarises the situation across EU Member States.



Green: no cash limits set – HU, PL: limits only apply to business-to-business transactions

The map below provides a graphical representation of the intensity of the cash limits set (from the darkest to the lightest blue), where they exist, and where countries without cash limits are located. The map shows that generally neighbouring EU countries have applied different thresholds or often taken different approaches (limit/no limit), which impacts on the effectiveness of the national measures.



In its Report to the European Parliament and the Council on restrictions on payments in cash of 12 June 2018[21], the Commission noted that introducing cash limits at EU level could have potential benefits on fighting money laundering. The report also concluded that diverging national provisions on payments in cash distort competition in the internal market, leading to potential relocations of businesses across borders, in particular for some specific sectors relying significantly on cash transactions, such as jewellery or car dealers. The report finally noted that diverging national restrictions potentially create loopholes allowing the bypassing of national cash payment limits, therefore decreasing their efficiency.

The Action plan for a comprehensive Union policy on preventing money laundering and terrorist financing, adopted by the Commission in May 2020, noted the different approaches taken by Member States to mitigate the ML/TF risks associated with cash. The Action Plan pointed out that the introduction of ceilings for large cash payments is one of the measures that could deliver a reinforced AML/CFT rulebook.

In reaction to the Action Plan, the Council conclusions of 17 June 2020 on enhancing financial investigations to fight serious and organised crime noted that the analytical work done by the Commission and Europol shows that criminals use cash payments to launder money and to finance terrorism. The conclusions called on the Commission to re-engage in a discussion with Member States on the need for a legislative limitation on cash payments at EU level.

Against this background, the Commission has proposed in its AML package published on 20 July 2021 a ceiling on cash payment. According to Commission's proposal[22], traders in good or services will be prevented from accepting cash payments of over EUR 10 000 for a single purchase, while allowing Member States to maintain in force lower ceilings for large cash transactions[23]. This ceiling does not apply to private operations between individuals. The Commission will assess the benefits and impacts of further lowering of this threshold within three years of application of the proposed Regulation.

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.

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

It must be noted that diverging national restrictions weaken the effectiveness of national cash threshold, by displacing illegal activities from a Member State with cash payment restrictions to a neighbour with more lenient restrictions or no restrictions at all. This was confirmed by anti-mafia prosecutors at the Commission's High-Level Conference on AML/CFT of 30 September 2020, who noted that the absence of cash ceilings in many EU Member States facilitates laundering of proceeds for organised crime across the EU.

[21] COM(2018)483 final.
[22] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM(2021)/420.
[23] The fact that there is no harmonised proposed way yet across Member States to deal with violations to the proposed threshold should also be assessed.

Threat

Terrorist financing

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.

Europol Financial Intelligence Public Private Partnership (EFIPPP) typologies:

Trafficking in human beings: Organised crime groups involved send cash/invest illegal profits in the country of origin: using cash couriers and MSBs (Western Union, MoneyGram) and / or invested in real estate, luxury vehicles and cash intensive businesses.

Infiltration of the legal economy: Outside the context of the pandemic, when infiltrating businesses, organised crime groups make wide use of cash and cash-intensive sectors; figureheads (of various nature); complex business ownership structures; off-shore countries and EU Member States with lower corporate transparency requirements.

Infiltration of the legal economy: the cash intensity of an economy, as well as possible limits on cash payments, are geographical indicators to determine the vulnerability to infiltration.

ML through real estate: The current economic climate following the second wave of Covid-19 pandemic and lockdown measures created new opportunities for criminals to invest in real estate or troubled businesses to generate cash and launder illicit proceeds. While the COVID-19 crisis has so far marginally affected the real estate market overall, disruption caused by lockdown measures and travel restrictions significantly impacted hotel, retail outlets and gastronomy sectors, resulting in reduced property prices and rendering real estate firms and economic operators in these sectors more susceptible to financial difficulties or other pressures, thus creating risk and potential weaknesses for criminals to exploit.

ML through real estate: the construction and renovation of real estate business are vulnerable to ML. Price settlements are usually made via unreported cash payments and there is involvement of recently created and/or obscure construction firms. In addition, different stakeholders (e.g. architects, construction site managers, construction workers) could assist in the laundering of illegal proceeds by not declaring payments or contributing to invoice falsification for tax evasion purposes. Use of low-paid, illegal workforce to under-declare costs and facilitate the laundering of the proceeds and/or commit tax fraud.

Illicit trade: while severe lockdown periods were imposed around the globe, the transnational criminal organisations that deal inter alia with illicit trade quickly adapted their modus operandi to make use of the new reality and supply markets additionally with illicit services and products that are in high demand during the pandemic. These include for instance substandard and falsified face masks, disinfectants and medicines associated with COVID-19 and tobacco products and drugs.

Illicit trade: the illegal trade in tobacco has risen considerably due to the COVID-19 pandemic.

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

Cash intensive business 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.

Law enforcement authorities 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

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 checks

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

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 checks

Pending the adoption of Commission's proposal[24] on cash ceiling by the European Parliament and Council, currently no upper limits to cash payments are in place at the EU-wide level.

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 due to the legal requirements which allow the refusal of cash payments above a certain threshold. In these cases, controls are in place and allow detecting red flags and suspicious transactions more easily. In addition, these cash payment thresholds are perceived by the sector and by LEAs as more efficient and, eventually, less burdensome than imposing customer due diligence measures. However, these legal businesses can also hide shadow and illicit activities which are able to circumvent 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 AML Directive to the extent that they make or receive cash payments of EUR 10 000 or more. 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.

This is the reason why the Commission has proposed in its AML package proposed on 20 July 2021 the introduction of a cash ceiling of EUR 10 000.

[24] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing COM(2021)/420.

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. As a result, subsequent information for investigations by 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as very significant (4).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant/very significant (level 4).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is HIGH and for money laundering VERY HIGH.

Mitigating measures

- Money laundering and terrorist financing risks have not been sufficiently mitigated by the requirement for traders in goods to be subject to anti-money laundering rules when making or receiving cash payment of EUR 10 000. At the same time, differences in approaches among Member States have created loopholes within the internal market. The Commission deems it therefore necessary to propose a Union-wide limit to large cash payments of EUR 10 000. Member States should be able to adopt lower thresholds and further stricter provisions to mitigate the risk of money laundering and terrorist financing.
- The Commission will continue to monitor the application of limits to large cash payments across Member States. According to Commission's proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing published on 20 July, the Commission intends to present by 3 years from the date of application of that Regulation a report assessing the need and proportionality of further lowering the limit for large cash payments.
- 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. 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. In that respect, Commission's proposal for a Directive on the mechanisms for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing allows Member States to extend the application of money laundering requirements to sectors not covered in the scope of the Regulation.

For this purpose, should the proposal be adopted, Member States will have to notify and explain their intention to the Commission that will adopt an Opinion on these plans.

- Considering the cross-border nature of ML and TF, Member States should seek international cooperation encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

3. High value banknotes

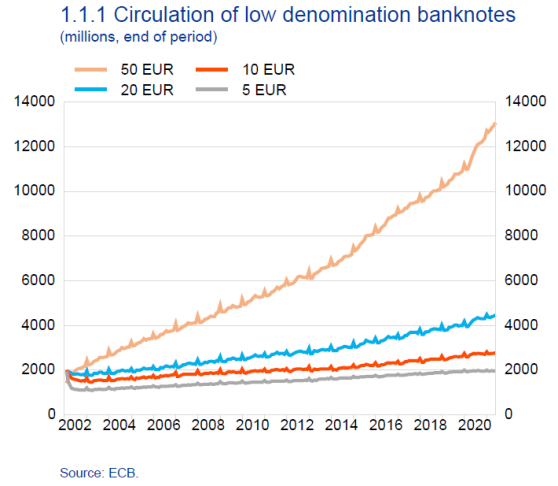
Product

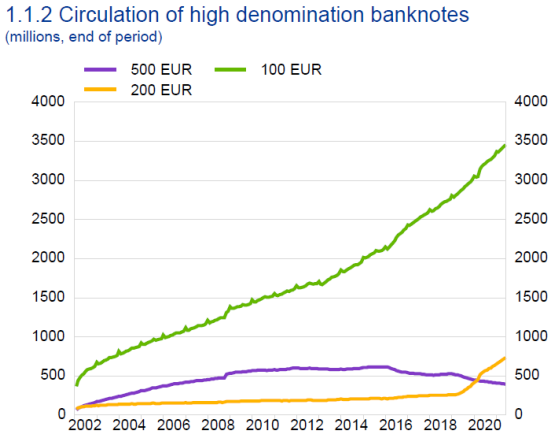
High value banknotes

Sector

In spite of a steady growth in non-cash payment 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. This trend is referred to as "the paradox of banknotes": the demand for euro banknotes has constantly increased while the use of banknotes for retail transactions seems to have decreased[25]. According to the ECB, this seemingly counterintuitive paradox can be explained by demand for banknotes as a store of value in the euro area (e.g. euro area citizens holding cash savings) coupled with demand for euro banknotes outside the euro area[26].

Cash is largely used for low value payments[27] and its use for transaction purposes is estimated to account for less than one-third of banknotes in circulation[28]. Meanwhile the demand for high denomination notes, such as the EUR 500 note, not commonly associated with payments, has been sustained in spite of the EUR 500 note not being issued anymore since April 2019. These are anomalies which may be linked to criminal activity.





There is insufficient information around the use of cash, 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. The ECB only provides broad estimates[29].

[25] "The paradox of banknotes : understanding the demand for cash beyond transactional use", ECB Economic Bulletin, Issue 2/2021.

[26] According to the ECB ("Foreign demand for euro banknotes", Occasional Paper Series, No 201, 2021), between 30% and 50% of the value of euro banknotes was held abroad in 2019 and this share has been increasing in recent years.

[27] See fiche on Cash intensive businesses. 33% of transactions above 100% which represent 3% of all POS and P2P transactions are paid in cash.

[28] According to ECB ("The paradox of banknotes: understanding the demand for cash beyond transactional use", ECB Economic Bulletin, Issue 2/2021), between 13% and 30% of the value of banknotes in circulation was held for the purpose of euro area transactions, yielding a central estimate of 21,5% (EUR 280 billion).

[29] The ECB uses statistic methods to estimate the use of euro banknotes for transactional use, for domestic store of value and for the circulation of euro banknotes outside the euro area. See "The paradox of banknotes: understanding the demand for cash beyond transactional use", ECB Economic Bulletin, Issue 2/2021. In 2019, between 13% and 30% of the value of banknote

While statistics exist on the volume and value of bank notes issued and in circulation in the EU, the question remains as to the use of a large proportion of cash in issuance especially when considering the EUR 500 note. The use of a significant proportion of banknotes remains unknown. Furthermore, the EUR 500 note accounts for 13,2% of the value of all banknotes in circulation, despite it not being a common means of payment. The EUR 200 and EUR 100 banknote account respectively for 10,2% and 23,5%[30]. 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.

As evidenced in the Chart 1.1.2 above, the EUR 200 banknote whose circulation has significantly increased tends to replace the EUR 500 banknote since 2019.

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[31] 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[32].

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).

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. Law enforcement authorities 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"

circulation was held for the purpose of euro area transactions. Between 27,5% and 50% of the value of banknote circulation is thought to be stored in the euro area in 2019. Regarding the circulation of euro banknotes outside the euro area, it has been estimated ("Foreign demand for euro banknotes", Occasional Paper Series, ECB, No 253, 2021) that between 30% and 50% of the value of euro banknotes was held abroad in 2019. This share has been increased in recent years.

[30] ECB Statistical Data Warehouse, June 2021.

[31] https://www.europol.europa.eu/newsroom/news/europol-welcomes-decision-of-ecb-to-stop-printing-eur500-notes

[32] Europol stresses that this is still a problem in the cases supported by the Agency and the question of stopping the use of EUR 500 bank notes could be raised.

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 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 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 is 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

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 checks

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

a) Risk exposure

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

b) Risk awareness

Especially LEAs and FIUs have high risk awareness, as do obliged entities subject to AML/CFT obligations. Risk awareness of sectors not covered by AML/CFT obligations or cash limitations obligations remains challenging. Existing literature, especially Europol reports, point to the blind spot in risk awareness (i.e. the precise use of high 27 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 checks

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.

Risk level

As regards **terrorist financing**, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as very significant (4).

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as very significant (level 4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔

Conclusions: estimated risk level for terrorist financing is HIGH and for money laundering VERY HIGH.

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.

- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

4. Payments in cash

Product

Payments in cash

Sector

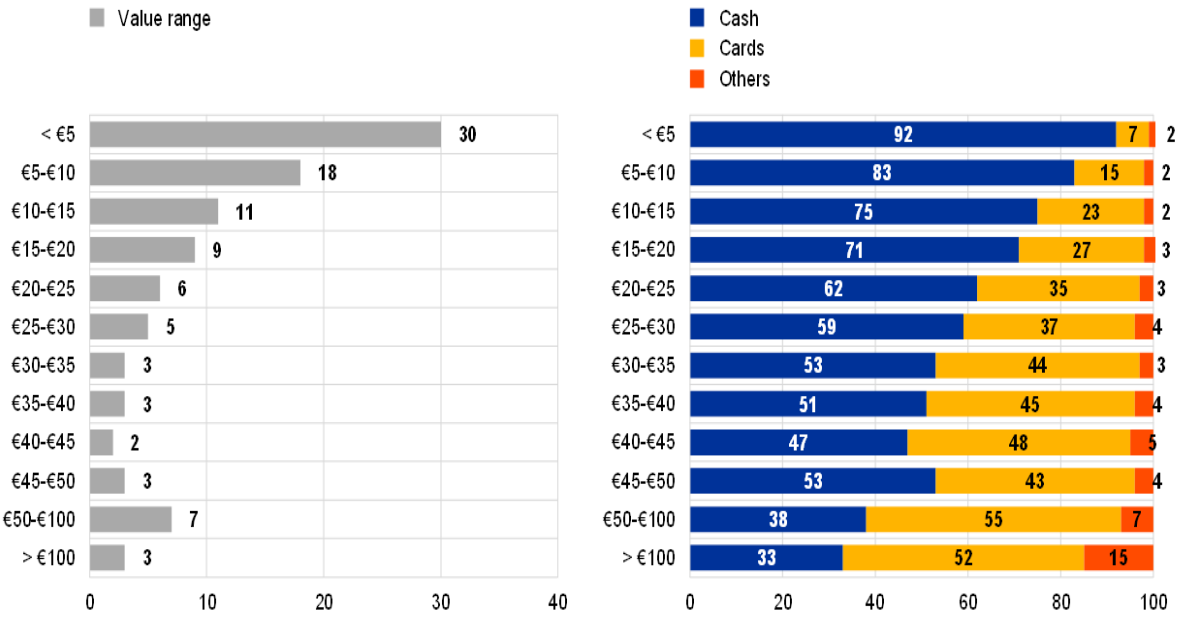
According to a December 2020 ECB's study on the payment attitudes of consumers in the euro area (SPACE)[33], consumers still predominantly use cash for Point of Sale (POS) and Person-to-person (P2P) payments:

- 73% of the volume of POS and P2P transactions was carried out using cash as a payment instruments;
- In value terms, cash transactions accounted for 48% of all transactions;
- Cash usage of 79% in terms of number of transactions.

The significant difference between number of transactions and value is due to the more frequent use of cash for low-value transactions. As shown in the ECB SPACE study, for both POS and P2P, payments below EUR 15 represent most of the transactions. 92% of payments below EUR 5 are made in cash while only 33% of transactions above EUR 100 (which represent only 3% of all POS and P2P transactions) are paid in cash.

Use of payment instrument at POS and P2P, by value range

(x-axis: percentage, share in all transactions; y-axis: value, transactions)



Sources: ECB, De Nederlandsche Bank, Dutch Payments Association and Deutsche Bundesbank

[33] https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf

While the increase in banknote circulation has been abnormally high during the COVID-19 pandemic[34], the use of cash payment has been only slightly impacted. According to ECB SPACE survey, almost half of the respondents reported that they used cards and cash in a similar way. Nevertheless, 40% of respondents used contactless payment more often and the same percentage of respondents declared that they used cash much less often or somewhat less often as they did before the start of the Pandemic.

Description of the risk scenario

This risk scenario is intrinsically linked to cash intensive business and high value denomination banknotes 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 small amounts of cash, terrorist activities without any traceability (see general description under cash intensive business).

In the European Supervisory Authorities' Joint Opinion of 2019, the risk deriving from the use of cash was one of the key concerns for competent authorities. According to EBA[35], the risk continues to be relevant for a much smaller proportion of competent authorities. Some competent authorities noted in that regard an increase in the use of contactless methods of payment, which has since been exacerbated in the current context of COVID-19.

Threat

Terrorist financing

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.

Europol Financial Intelligence Public Private Partnership (EFIPPP) information/ indicators extracted from typologies:

Infiltration in legal economy typology:

- The cash intensity of an economy, as well as possible limits on cash payments, are geographical indicators to determine the vulnerability to infiltration.

[34] See Fiche on high value banknotes

[35] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector, March 2021

ML through real estate typology:

- Purchases, rental payments, return of deposit made in cash or monetary instruments, sometimes in combination with unusual advanced payments.
- Bank accounts opened in the name of non-financial professionals in order to carry out various financial transactions (e.g. depositing cash, issuing and cashing cheques, sending and receiving international fund transfers).
- Criminals may use illicit cash to acquire cheap real estate in crisis-hit (COVID-19) sectors as a cover to move funds or aiming at the economic exploitation of the property or subsequent sale due to expected price increases.
- Payment for construction of renovation of real estate via unreported cash payments. Also rental payments or return of deposits in cash.

Illegal trade typology:

- Regarding the illegal trade in tobacco, an indicator is that payments are made to unrelated third parties via: i) Cash. ii) Wire transfers. iii) Checks, bank drafts or postal money orders from unrelated third parties. Cash based payments are also used in illegal wildlife trade.

Conclusions: Based on the feedback from LEAs 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

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 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 checks

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[36]. 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.

Against this background, in its proposal for an AML package presented on 20 July 2021, the Commission has proposed to prevent traders in good or services from accepting cash payments of over EUR 10,000 for a single purchase, while allowing Member States to maintain in force lower ceilings for large cash transactions. This ceiling does not apply to private operations between individuals. As a consequence of the introduction of cash limits, traders in goods would be removed from the list of obliged entities. Going forward, the Commission will assess the benefits and impacts of further lowering this threshold within three years of application of the proposed Regulation.

It must be noted that 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

[36] See fiche n.2 on "cash intensive business".

controls is not efficient), the level of TF vulnerability related to payments in cash is considered as very significant (level 4).

Money laundering

a) Risk exposure

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

b) Risk awareness

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

c) Legal framework and checks

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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as very significant (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant/very significant (level 4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, terrorist financing and money laundering is VERY HIGH.

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.
- The prohibition of payments in cash for some types of dangerous products – like those included in national databases on dangerous chemical products – should be considered.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

In the Commission proposed AML Regulation[37] , Member States will keep the possibility to extend the scope of application to other sectors not covered in the scope of that Regulation. For this purpose, Member States would have to notify and explain their intention to the Commission and suspend the effect of such extension for 6 months, during which time the Commission will adopt an Opinion on the plans. The Commission may then choose to propose legislation at Union level.

[37] COM/2021/420 final.

5. Privately owned ATMs

Product

Privately owned ATMs Sector

Sector

There exists a growing use of privately owned cash machines (ATMs) across the Union and its possible misuse 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.

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' side legal business[38] is running an MSB or a currency exchange service, the risk of misuse can be clearly identified. In addition, privately owned ATM may be used to purchase virtual currencies[39].

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[40]. 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.

[38] See the section on "Illegal transfer of funds - Hawala".

[39] https://www.justice.gov/usao-cdca/pr/oc-man-admits-operating-unlicensed-atm-network-laundered-millions-dollars-bitcoin-and

[40] Either a criminal organisation is the service provider and the ATMs exclusively loaded with proceeds of crime, or there exists a collaboration between service provider and criminal organisation, or it is a case of infiltration.

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. This hampers the proper monitoring by banks.

A review of the companies offering private ATM services shows that there are several major suppliers, British and American[41] who have managed to make their business international[42].

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.

Threat

Terrorist financing

There exist currently few specific 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).

[41] 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.

[42] 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.

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. This modus operandi is also used to purchase virtual currency, as reported by FIUs and confirmed by EUROPOL: As there exists not harmonised or control of crypto-ATM, it is easy to deposit cash in those crypto ATM to transform cash into crypto[43].

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

Vulnerability

Terrorist financing

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 checks

According to the EU legal framework, the service of cash withdrawal can be offered by unregulated entities (i.e. not subject to AML/CFT requirement). 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).

Money laundering

a) risk exposure

The vulnerability assessment of money laundering 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.

[43] Crypto-ATMs are dramatically flourishing over the world: https://coinatmradar.com/

c) legal framework and checks

According to the EU legal framework, the service of cash withdrawal may be offered by unregulated entities (i.e. not subject to AML/CFT requirement). 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 money laundering vulnerability is considered as very significant (level 4).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as very significant (4).

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant/very significant (level 4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔

Conclusions: estimated risk level for both, terrorist financing and money laundering is VERY HIGH.

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.
- An enhanced collaboration with customs agency will help acquire further information on the importation of AML machines.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

FINANCIAL SECTOR

1. Retail banking sector

Product

Retail deposits on accounts (excluding private banking)

Sector

Credit and financial institutions

General description of the sector and related product/activity concerned

European Union total deposits was reported at EUR 14,8 billion in October 2021[44]. The data reached an all-time high of EUR 15,3 billion in May 2021 and a record low of EUR 3,7 USD billion in October 2000. This is the sum of all deposits by non-financial corporates, households, insurance corporates, pension funds and other financial intermediaries, which covers all Monetary Financial Institutions (MFIs).

In Euro area, the European Central Bank reported the total of EUR 8,665.6 billion of deposits vis-à-vis other Euro area residents in Q3 of 2021[45]. This figure similarly includes both retail and corporate deposits.

In terms of trends, the global pandemic has driven an increase in savings by households, which is reflected in the increase of the total deposits from around EUR 12,4 trillion in January 2020 in the wake of the pandemics to current EUR 14,8 trillion in Q3 2021. The level of deposits has only started to decrease in May 2021, reflecting a tentative return to normalised consumer spending behaviour.

Description of the risk scenario

Money launderers 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.

Natural persons may open bank accounts based on fake identification documents. Usage of such bank accounts to collect and transfer money from illegal sources (i.e. to introduce resources to the banking system and to further transfer these).

[44] https://www.ceicdata.com/en/indicator/european-union/total-deposits
[45] https://sdw.ecb.europa.eu/reports.do?node=1000003156

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 not only by terrorists, but also by their relatives/friends; this extends the scope of the intent and capability analysis[46]. 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, 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. 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, deposits accounts are 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 and related money value transfer services 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 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[47]. Law enforcement authorities

[46] The intent and capability analysis is described in the methodology section ("Annex 2"):

- 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.

[47] See previous footnote.

report frequent use of this method as 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 accounts 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 most straightforward and least sophisticated 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.

c) legal framework and checks

Deposits on accounts have been included in the scope of 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 some banks limit them to sanctions screening, which is an element of, but 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 volume of deposits where, in the case of cash, the origin of funds cannot be always traced, is relatively high. 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. The inherent risk deposits on accounts can also be increased by the use of new technologies and non-face-to-face business relationships.

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 institutions 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. At the same time, in accordance with Study on EU Payment

Accounts Market , 55% of the respondents answered that the suspicion of money laundering or terrorism financing was a key reason for refusing customers the opening of a payment account[48].

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, 2020 was the year when record amount of AML/CFT compliance-related fines were issued in the financial sector globally, and another record for fines in the Union banking sector[49].

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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as significant.

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
➔	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as significant (3), and the level of vulnerability has been assessed as very significant (level 4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is 3, HIGH, and the estimated risk for money laundering is 4, VERY HIGH.

Mitigating measures

For the Commission:

- Introduction of a harmonised, directly applicable framework of customer due diligence requirements, including remote on boarding requirements.

[48] https://op.europa.eu/en/publication-detail/-/publication/5bec1d2b-65d2-11eb-aeb5-01aa75ed71a1/language-en (see Figure 4 and page 13-14).
[49] https://www.kyckr.com/aml-bank-fines-2020/

- Introduction of harmonised requirements for identification of beneficial owners and a harmonised framework of requirements applicable to beneficial owners and their associates.
- Introduction of Union-wide large cash payments limit of EUR 10 000.
- Collect and promote best practices in the area of 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 limits on cash transactions currently in force in the Member State 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.
    - 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.

2. Retail and institutional investment sector

Product

Retail and institutional investment products and services

Sector

Financial institutions – credit institutions, asset management companies, investment firms

General description of the sector and related product/activity concerned

The EU asset management sector can be subdivided into three categories. The first category comprises the mutual fund industry, the Undertakings for Collective Investment in Transferable Securities ('UCITS') funds (11.6 trillion euros of net assets domiciled in Europe under management in 2020). The second category includes alternative investment funds ('AIFs') (the alternative investment fund industry had a net asset value of 7.1 trillion euros at the end of 2020) such as hedge funds, private equity, funds of funds and real estate funds. The third subcategory relates to discretionary mandates. Altogether, the asset management sector has steadily increased which is reflected by the fact that 27 trillion euros (or 157% of European GDP) of European Assets are estimated to be managed by the first quarter of 2021, 55% on behalf of investment funds and 45% in managing discretionary mandates.

Total fund ownership in Europe which relates to the funds that are bought and held by investors in Europe and excludes funds domiciled in Europe that are sold outside Europe has also been steadily growing. For instance, there has been an increase to 13.6 trillion euros at the end of 2020, compared to 6.3 trillion euros in 2010. The highest levels of fund ownership can be found in Germany, France, the Netherlands and Italy.

Overall, there are more than 4,500 asset management companies operating in Europe with most of the activity taking place in the United Kingdom, France, Germany, Switzerland, Italy and the Netherlands. In terms of domiciles, Luxembourg and Ireland are leading with market share in 2020 of 27% and 18%, respectively.

The EU asset management industry serves both retail clients — usually composed of households and high net worth individuals — as well as institutional clients. Institutional clients which include insurance companies and pension funds, still account for the largest stake of investment funds held with 74.7% while households account for 25.3%[50].

Description of the risk scenario

There are various scenarios where criminals can commit abuses against investors or financial markets resulting in, or amounting to, money laundering. For instance, criminal proceeds may be used to purchase investment products (e.g. using brokerage accounts), such as title of shares to conceal beneficial ownership, investment activity may be used to justify criminal proceeds such as profit obtained from other (illicit) activity Predicate investment fraud, or placement of proceeds using specialised high-return financial services, and market abuse (which comprises insider dealing, market manipulation, and unlawful disclosure of inside information, all of which are covered by the scope of

[50] https://www.efama.org/about-our-industry/our-industry-numbers

the EU Market Abuse Regulation[51] and the EU Criminal Sanctions for Market Abuse Directive[52]), are also examples of money laundering risk scenarios.

General comments

The main risk scenario considered from the perspective of money laundering vulnerability is linked to intermediated investment services

Threat

Terrorist financing

The terrorist financing threat related to retail and 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.

Conclusions: 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 involved in investment-related activities, they are not easy to access, the investment activities themselves not necessarily financially viable (depending on the quality of investment) and in any case requires knowledge and technical expertise. Therefore, criminal organisations usually abstain from carrying out investment activities themselves[53], which makes the role of facilitators essential for both creating and utilising opaque structures to hide the proceeds of criminal activities.

A few methods for moving large illicit flows, prepared by highly skilled facilitators, have remained relevant:

- capital market commodity participants conducting over-the-counter future swaps[54] 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 participants conducting bond trades on behalf of organised criminals, using illegitimate money to purchase bonds and then deposit funds into financial institutions after sale of those bonds.

[51] 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.*

[52] 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.*

[53] Although there may be exceptions, see https://www.amlc.eu/private-investment-funds-and-money-laundering/

[54] Unlike most standardized options and futures contracts, swaps are not exchange-traded instruments. Instead, swaps are customized contracts that are traded in the over-the-counter (OTC) market between private parties. Because swaps occur on the OTC market, there is always the risk of a counterparty defaulting on the swap.

Conclusions: in this context, the assessment of the money laundering threat related to retail and institutional investment services, especially involving facilitators/brokers is considered as significant (level 3).

Vulnerability

Terrorist financing

Terrorist financing vulnerability related to investment services presents a less significant inherent risk. Risk factors (products, customers, geographies and delivery channels) do not favour the use of this products and services for terrorist financing purposes.

Perpetrators usually do not have the expertise to access the sector, while the low amounts of money used to finance terrorist attacks made other sectors more attractive for their purposes.

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

Money laundering

The assessment of the money laundering vulnerability related to retail and institutional investment sector is as follows:

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 investment sector, perpetrators need to introduce money through the banking system, and hiding illegal money through opaque structures requires a high degree of expertise and/or high cost. Therefore, banks are often 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 potential 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, where the investment service is intermediated, the level of vulnerability to money

laundering is higher than the vulnerability of retail or institutional investment services provided directly to the end client.

c) legal framework and checks

Institutional and retail investments services through all types of financial sector entities 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 reduce incentives to carry out rigorous 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 potentially illegal proceeds are introduced into financial system via banks. When investment services involve intermediation by brokers, money laundering vulnerability is higher than when those services are directly to end customers. In addition, 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. 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 investment services provided through brokers is considered as moderately significant/significant (level 2/3).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as non-relevant (1>).

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant/ significant (level 2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for money laundering is HIGH.

Mitigating measures

For the Commission:

- Introduction of a harmonised, directly applicable framework of customer due diligence requirements for all the relevant types of financial sector obliged entities active in the area of retail and institutional investment services.

- Introduction of a harmonised requirements for identification of beneficial owners and harmonised framework of requirements applicable to beneficial owners and their associates.
- Establishment of the interconnection of beneficial owner registers at EU level.

For Member States / competent authorities:

- Effective implementation 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.
- Thematic inspections to assess:
    - effectiveness of customer due diligence and enhanced customer due diligence as well as beneficial owner identification requirements are implemented by financial sector entities providing retail and institutional investment services.

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.

3. Corporate banking sector

Product

Corporate banking products (including trade finance)

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 to carry out individual terrorist attacks and other products/sectors which are less traceable may be utilised. Individuals who would wish to finance terrorist activities do not prefer these type of products, and there is currently a lack of evidence to suggest that terrorist organisations are using corporate banking services in the EU. Therefore the terrorist financing threat is not significant in this product/sector.

Conclusions: 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 is plausible. However, using corporate banking for money laundering requires more sophistication than the retail financial sector. Specifically, using corporate banking products or services for money laundering would require the complicity of financial/legal intermediaries who need to be paid for their 'services'. There is evidence of the risk posed by such intermediaries.[55]

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).

[55] https://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar-crime.pdf

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. Individual 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.

Conclusions: 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'.

b) 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, the sector complains about the 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.

c) 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 and geographical areas, and to a lesser extent associated with products and transactions. 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as low (1).

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant/significant (level 2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is 1, LOW, and for money laundering is 3, HIGH.

Mitigating measures

For the Commission:

- Introduction of a harmonised, directly applicable framework of customer due diligence requirements.
- Introduction of a harmonised requirements for identification of beneficial owners and harmonised framework of requirements applicable to beneficial owners and their associates.
- Establishment of the interconnection of beneficial owner registers at EU level.

For Member States / competent authorities:

- Effective implementation 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.
- Authorities should provide more substantive feedback on the submitted suspicious activities and transaction reports, organise 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.

4. Private banking sector

Product

Private banking and wealth management products and services

Sector

Credit institutions

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 all private banking and wealth management services for integration of criminal proceeds. Given the combination of sophisticated financial products and services, and a wealthy customer base, which sometimes includes politically exposed persons (PEPs), the sector can be abused also for tax evasion, especially in cases where assets of the beneficial owners are hidden behind complex ownership structures and direct private banking customers are the associates or family members of the actual beneficial owners.

General comments

For this risk scenario, financial services concern services provided to high net worth individuals only.

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. Nevertheless, wealthy terrorism sponsors might enter into asset or wealth management agreements with private banks with a view to harbouring their assets even though their assets or wealth under management might not be related directly to TF.

Conclusions: not relevant

Money laundering

The assessment of the money laundering threat related to private banking (wealth management) shows that this sector is most often 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 of assets under wealth management 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 necessarily have equivalent AML/CFT regimes to the EU AML/CFT framework.

b) risk awareness

According to financial intelligence units, private banking is characterised by a very low (almost non-existent) level of suspicious transaction reporting. As for private banking-related 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 net worth individuals (who often demand high level of secrecy and discretion conflicting with AML/CFT CDD

requirements) as 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as non-relevant.

RISK	
1 – 1,5	
1,6 – 2,5	
2,6 – 3,5	
3,6 – 4	

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant/very significant (level 3/4).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for money laundering is 3, HIGH.

Mitigating measures

For the Commission:

- Introduction of a harmonised, directly applicable framework of customer due diligence requirements, including enhanced customer due diligence requirements related to Politically Exposed Persons and/or high-risk third country jurisdictions.
- Introduction of a harmonised requirements for identification of beneficial owners and harmonised framework of requirements applicable to beneficial owners and their associates.
- Establishment of the interconnection of beneficial owner registers at EU level.

For Member States / competent authorities:

- Effective implementation 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.
- 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.

5. Crowdfunding

Product

Crowdfunding

Sector

Crowdfunding platforms

Description of the risk scenario

Crowdfunding service providers have different crowdfunding models, carrying different level of money laundering and terrorist financing risks. For instance, the activities to collect funds for later onward transmission are particularly vulnerable to money laundering, notably where the funds collected for an undetermined project remain in the investor's account until the project is formaklly determined. Donation platforms can also be misused to disguise the illicit origin of funds or for TF purposes[56]. Perpetrators can also use platforms to collect/accumulate funds and transfers them abroad. As of 10 November 2023, the Regulation on European Crowdfunding Service Providers (ECSP) for business[57] will be in application and will require all payment be carried out through an authorised Payment Service Provider (PSP) as well as introduced other safeguards to mitigate these risks. There will however still be platforms operating in sectors not regulated under EU law, for example donation or reward-based crowdfunding platforms. Crowdfunding platforms, which are unregulated, could be set up under fictitious projects in order to allow collection of funds which are then withdrawn within the EU or transferred abroad, potentially for ML purposes or to finance terrorist attacks. This could be used either to collect funds from legitimate sources for the purpose of terrorist financing – or to collect illicit funds from criminal activities using anonymous products. ECSPs that collect funds for later onward transmission are particularly vulnerable to money laundering, including business models where the funds are collected for an undetermined project and consequently held in the investor's account until the project is determined.

Threat

Terrorist financing

Terrorist groups may have the intent to use the crowdsourcing techniques to collect funds. Unregulated crowdfunding platforms may be used to fund fictitious investment projects with illicit funds or being misused for TF purposes where a fictitious reason is given for a crowdfunding project, which never materialises and the funds obtained from crowdsourcing are thereafter used for terrorist financing purposes. Overall, law enforcement authorities reported some 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

[56] EBA report on money laundering and terrorist financing risk affecting the EU financial sector of 3 March 2021, page 22.
[57] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (Text with EEA relevance); *OJ L 347, 20.10.2020, p. 1–49.*

agencies is identifying the end recipient and the use of the donations (proof of terrorist financing). Risks are also increased due to the borderless nature of platforms given that potential donors can be located anywhere in the world, including in high-risk jurisdictions.

Europol Financial Intelligence Public Private Partnership (EFIPPP), general input on donations from the typology on Match-fixing/betting, case example:

A transnational organised crime group focused on money laundering through the football sector identified football clubs in financial distress and infiltrated it 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.

Conclusions: Law enforcement agencies have evidence of terrorist groups having used 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 are different ways for criminals to use Crowdfunding platforms to actually launder the proceeds of crime. Thus, poorly supervised or unregulated Crowdfunding platforms could be vulnerable to being abused for ML purposes in case of collusion between the project owner and investor for fictitious projects. National competent authorities note that this risk was high as long as it was relatively easy to launch and market a crowdfunding project and the use of criminal intermediaries could make the sector more attractive for money laundering purposes. However, the Regulation on European Crowdfunding Service Providers (ECSP) should enhance the monitoring of the ECSPs and limit their misuses risk once it will be in force and law enforcement agencies consider that risks relating to crowdfunding platforms remain low, with some signs of instances where they could have been used 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.

The level of risk exposure varies depending on whether crowdfunding is directly linked to financial institutions or left to private initiatives on the internet. The risk is higher if crowdfunding platforms use virtual currencies or (anonymous) electronic money. Depending on the type of platform vary TF risk as well, the riskier platforms for TF are donation platforms which are out of the scope of financial institutions and out of the AML legal framework.

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 providers 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

Legal divergence in this area is until now a major source of concern, and the absence of a harmonised framework setting out clear AML/CFT obligations applicable to crowdfunding platforms significantly increases the EU's exposure to ML/TF risks. Crowdfunding platforms as such are not obliged entities under the AMLD, and while some Member States have included CFPs in their national legislation transposing the AMLD, not all Member States consider crowdfunding platforms as obliged entities[58]. Regulation (EU) 2020/1503 of the European Parliament of the Council on European Crowdfunding Service Providers for business[59] harmonises the regulatory approach for business investment and lending-based crowdfunding platforms across the Union and ensures that adequate and coherent safeguards are in place to deal with potential money laundering and terrorist financing risks. Among those, there are requirements for the management of funds and payments in relation to all the financial transactions executed on these platforms. Crowdfunding service providers must either seek a license or partner with a payment service provider or a credit institution, which are obliged entities under this Regulation, for the execution of such transactions. The Regulation also sets out safeguards in the authorisation procedure, in the assessment of good repute of management and through due diligence procedures for project owners. The Commission will assess by 10 November 2023 in its report on that Regulation whether further safeguards may be necessary. It is therefore justified not to subject crowdfunding platforms licensed under Regulation (EU) 2020/1503 to EU AML/CFT legislation.

Crowdfunding platforms that are not licensed under Regulation (EU) 2020/1503 are currently left either unregulated or to diverging regulatory approaches, including in relation to rules and procedures to tackle anti-money laundering and terrorist financing risks. To bring consistency and ensure that there are no uncontrolled risks in such environment, the European Commission envisages to add the crowdfunding platforms that will not be licensed under Regulation (EU) 2020/1503 to the obliged entities of the EU

[58] According to EBA report on money laundering and terrorism financing risks affecting the EU's financial sector, 12 Member States were still not considering any crowdfunding platforms as obliged entities in 2019: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

[59] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937; *OJ L 347, 20.10.2020, p. 1.*

AML/CFT framework[60]. It is therefore reasonable to expect to have a more comprehensive and enhanced legal framework for crowdfunding platforms in the coming years.

For the time being however, some 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 yet fully harmonised because a new cross-cutting framework dealing with this issue is currently being put in place, which will improve the situation. There are still 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, crowdfunding 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

Regulation (EU) 2020/1503 of the European Parliament of the Council on European Crowdfunding Service Providers for business[61] harmonises the regulatory approach for business investment and lending-based crowdfunding platforms across the Union and ensures that adequate and coherent safeguards are in place to deal with potential money laundering and terrorist financing risks. Among those, there are requirements for the management of funds and payments in relation to all the financial transactions executed on these platforms. Crowdfunding service providers must either seek a license or

[60] European Commission proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM/2021/420 final.
[61] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937; *OJ L 347, 20.10.2020, p. 1.*

partner with a payment service provider or a credit institution, which are obliged entities under this Regulation, for the execution of such transactions. The Regulation also sets out safeguards in the authorisation procedure, in the assessment of good repute of management and through due diligence procedures for project owners. The Commission will assess by 10 November 2023 in its report on that Regulation whether further safeguards may be necessary. It is therefore justified not to subject crowdfunding platforms licensed under Regulation (EU) 2020/1503 to EU AML/CFT legislation.

Crowdfunding platforms that are not licensed under Regulation (EU) 2020/1503 are currently left either unregulated or to diverging regulatory approaches, including in relation to rules and procedures to tackle anti-money laundering and terrorist financing risks. To bring consistency and ensure that there are no uncontrolled risks in such environment, the European Commission envisages to add the crowdfunding platforms that will not be licensed under Regulation (EU) 2020/1503 to the obliged entities of the EU AML/CFT framework[62]. It is therefore reasonable to expect to have a more comprehensive and enhanced legal framework for Crowdfunding platforms in the coming years.

For the time being however, 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).

Risk level

As regards terrorist financing, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as moderately significant (2).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as moderately significant (2).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, money laundering and terrorist financing, is level 2, MEDIUM.

[62] European Commission proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM/2021/420 final.

Mitigating measures

In its legislative proposal the Commission has added as obliged entities "crowdfunding service providers other than those regulated by Regulation (EU) 2020/1503".

For the competent authorities:

- Member States should consider the need to define unregulated crowdfunding platforms as complementary obliged entities subject to AML/CFT requirements.
- Member States should closely monitor the legal developments related to the treatment of crowdfunding services providers and crowdfunding platforms for AML/CFT purposes.
- Member States should assess risks associated with crowdfunding in their jurisdiction, even where crowdfunding services providers and crowdfunding platforms are not obliged entities, as these risks may have an impact on regulated services.
- Member States should consider further communication to set out clearly their regulatory expectations in respect of the sector as well as the risks to which crowdfunding services providers and crowdfunding platforms are exposed[63].
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

For the sector:

- Crowdfunding services providers (CSPs) should know their customers to prevent their crowdfunding platforms from being used to fund fictitious investment projects with illicit funds or being misused for ML or TF purposes.
- Crowdfunding services providers should take into account, among others[64], the following risk factors as potentially contributing to increased risk when performing customer due diligences:
    - business models where funds are collected through the crowdfunding platform but allows for later onward transmission (including where money is collected for an undetermined project and consequently held in the investor's account until the project is determined; or where money is collected but may be returned to the investors where the fundraising target is not met, or where the project owner has not received the money);
    - business models allowing early redemption of investments, early repayment of loans, or resale of the investments or loans through secondary markets;
    - the absence of restriction on the size, volume or value of the transactions, loading or redemption processed through the crowdfunding platform, or the amount of funds to be stored in individual investor accounts;
    - the possibility for investors to make payments through the crowdfunding platform with instruments not regulated or subject to less robust AML/CFT requirements than those required by Directive (EU) 2015/849.

[63] Member States may notably refer to EBA's Risk-based Supervision Guidelines: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1663861/7159758d-8337-499e-8b12-e34911f9b4b6/Joint%20Guidelines%20on%20Risk-Based%20Supervision%20%28ESAS%202016%2072%29.pdf?retry=1

[64] See EBA's Risk Factors Guidelines: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

6. Currency exchange

Product

Conversion of funds

Sector

Currency exchange offices (Bureaux de change)

Description of the risk scenario

Perpetrators are converting their funds into another currency to facilitate the conversion, transfer or laundering of funds[65]. Currency exchange offices can be used for money laundering purposes either by performing relevant transactions without knowledge of the illegal origin or destination of the funds concerned or by a direct involvement of the staff/management of the provider through complicity or takeover of such businesses by the criminal organisation[66]. Currency exchange offices are usually key nodes with the money laundering controller networks.

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.

Europol Financial Intelligence Public Private Partnership (EFIPPP) information based on typologies: Services of ML Controller Networks (MLCNs) include 'cash swap': cash is collected in a currency and paid out in another currency, including cryptocurrency.

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 exchange office method is highly suitable to achieving money laundering objectives. In particular, the launderer can employ the office either as an operator or customer. The former is riskier; however, it facilitates an integration, whereas the latter is only applicable to the placement or the preparation of

[65] As an overview: FATF (2010), *Money Laundering through Money Remittance and Currency Exchange Providers*.
[66] As an example: https://www.europol.europa.eu/newsroom/news/operational-task-force-leads-to-dismantling-of-one-of-europe's-most-prolific-crime-groups-behind-€680-million-operation, 22.05.2019.

a placement. If the money launderer desires to launder smaller amounts of money on an irregular basis, they may frequent the office as a customer or send a straw man.[67]

The most adequate placement should be in a city with many tourists holding different currencies from various nations. 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.

Currency exchange offices could also be part of a cash pool in a money laundering controller network.

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 always 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

[67] Teichmann, F. and Falker, M-C. (2019), "Money laundering through exchange offices", *Journal of Money Laundering Control*, 20.01.2020.

poor, similar to checks related to customer identification and verification[68]. 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, operate out of the same premises, or even the same employee takes charge of both transactions. 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

[68] Many transactions are occasional transactions under the threshold for a complete identification of the customer. Split transactions are difficult to identify when mules or multiple exchange offices are used to stay under the threshold.

countries to apply customer due diligence obligations only for occasional transactions; in any case, most Member States apply thresholds lower than EUR 15,000.

Conclusions: 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).

Risk level

As regards terrorist financing, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, money laundering and terrorist financing, is level 3, HIGH.

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 or currency exchange 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. An alternative option could be to impose a complete identification of customers doing several exchange transactions in a limited period (3-5 consecutive days). Some operators already applied such mechanism to monitor suspicious transactions.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

For the sector:

Technology assists the industry to meet compliance requirements set out by the regulator: some exchange business rely on cameras connected into a database, which alert authorities in case a listed, or even non-habitual, person is recognised. Systems for scanning photo ID documents can already indicate whether ID documents presented for the transaction are valid.

- Compliance should be accompanied by the implementation of **suitable CDD mechanisms** to accurately establish the identities of customers, and of **transaction monitoring and screening measures**.

- Transaction monitoring and screening measures should be focused on identifying high-risk customers and transactions, characterized by “red flag” behaviours and activities like, for instance:
    - Suspicious transactions patterns or transactions taking place in unusual circumstances.
    - Transactions through non-face-to-face services.
    - Possible indications on agents or mules being used to conduct transactions on behalf of a third party.
    - Customers who falsify or conceal their identities.
    - Cases of multiple connected transfers in different currencies or into and out of different countries.
    - Transactions to high risk third countries known to be major international and regional financial centres and trading hubs where many bureaux de change are situated, such as UAE and Hong Kong.
    - Customers who are politically exposed persons (PEPs), or who are on sanctions lists.

7. 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. 'Electronic money institutions' are legal persons that have been granted authorisation under E-Money Directive requirements to issue electronic money, they are also considered as obliged entities submitted to Directive (EU) 2015/849 (AMLD) as modified by directive 2018/843. 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 'software-based'. Most e-money products require identification of the owner, however some products benefit from the exemptions under the AMLD, which 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 is the manner in which e money is created or issued. The key distinction relates to whether e-money is 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 are 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 with 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, to the extent such instruments meet the conditions to fall under the limited network exemption in the EMD. Also, virtual assets 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 2019, the value of e-money payment transactions with e-money issued by resident PSPs - from EU amounted to EUR 195,8 billion[69]. The same year, the value of e-money payment transactions with e-money issued by resident PSPs - from Luxembourg (hosting PayPal and Amazon) amounted EUR 143,674 billion[70], while reaching EUR 36,6 billion in Italy[71] and only EUR 0,9 billion in Germany and EUR 0,561 billion in France. The average transaction value on that basis was of EUR 42. The number of e-money payment transactions - with e-money issued by resident PSPs from EU in 2019 was 4,66 billion[72] (including EUR 3,35 billion in Luxembourg, some EUR 0,98 billion in Italy but only 61 million in France and 33 million in Germany). The number of e-money payment transactions with e-money issued by resident PSPs from EU reached EUR 4,66 billion in 2019[73]. In the five-year period from 2015-2019, the number of e-money payment transactions with e-money issued by resident PSPs from EU increased by 95,7% (EUR 2,38 billion in 2015). These data are however not complete as they do not include several non-euro area markets and therefore underestimate the actual size of the EU market.

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.

[69] European Central Bank - Statistical Data Warehouse: https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.D0.F200.I50.Z00Z.VT.X0.20.Z01.E
[70] European Central Bank - Statistical Data Warehouse: https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.LU.F000.IEM.Z00Z.VT.X0.20.Z01.E
[71] European Central Bank - Statistical Data Warehouse: https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.IT.F000.IEM.Z00Z.VT.X0.20.Z01.E
[72] European Central Bank - Statistical Data Warehouse: https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.D0.F000.IEM.Z00Z.NT.X0.20.Z0Z.Z
[73] European Central Bank - Statistical Data Warehouse: https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.D0.F000.IEM.Z00Z.NT.X0.20.Z0Z.Z

This sector appears to be highly concentrated, with the majority of e-money issuers within the EU based in Belgium, the Czech Republic, Denmark, Latvia and the Netherlands. Outside of the EU, the United Kingdom is also a major market for the industry. 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 most frequently 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[74].

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. It is also to be noted that some cards can still be loaded with cash, which increases the risk of ML. It is only when money stored in cards is used that e-money issuers have a chance to trace or monitor transactions.

Threat

The main contributing factors that expose the sector to ML/TF risks are those associated with distribution channels, as the use of intermediaries in the distribution chain can make it more difficult to perform adequate AML/CFT controls and oversight. Other risks factors according to national competent Authorities are linked to the sector's extensive reliance on non-face-to-face identification processes (with increased risks of computer fraud and use of false documents), the relative anonymity of the customer for some of the products benefitting from exemptions under the AMLD, the ease and speed of e-money transactions and the poor overall awareness of ML/TF risks[75].

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

[74] 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://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/da05ad8a-eed2-410a-bd08-072403d086f3/EBA%20Opinion%20.pdf

[75] EBA Opinion on ML/TF risks, 3 March 2021, paragraphs 96 and 97: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

(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 as some e-money issues have placed restrictions on certain geographical areas where the cards can be used.

Law enforcement authorities 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 may have better traceability than cash, however, considering the speed of transactions and the possibility to physically transport the cards to jurisdictions designated as high risk for terrorism, even when the transactions are traced, it may be difficult to track the perpetrators. The level of threat is independent of the thresholds for applying customer due diligence if perpetrators are not included in sanction lists.

Europol Financial Intelligence Public Private Partnership (EFIPPP) typology information:

Misuse of Public Funds: Government payments are channelled to prepaid cards that are eligible to process and receive direct-deposit payments even a few days earlier before the payment is due (in US).

Non-delivery scam: The merchant requests payments that are unusual for the type of transaction in question or unusual for the industry's pattern of behaviour. For example, instead of a credit card payment, the merchant requires a pre-paid card, the use of a money services business, convertible virtual currency, or that the buyer send funds via an electronic funds transfer to a high-risk jurisdiction

Counterfeit goods: Financial products being used are a) E-Money and payment accounts (incl. virtual IBANs), b) Credit cards and pre-paid cards, c) Bank accounts (incl. virtual IBANs), d) Virtual assets. Virtual Assets Service Providers (VASPs) are amongst the "financial institutions" used.

Match-fixing/betting: electronic payment methods are used to open betting accounts online. Widespread use of cash couriers, money service businesses and increasingly e-wallets payment service providers to transfer the proceeds of crime linked to sports corruption cases and to fuel online betting accounts for large-scale match-fixing operations.

Corruption and bribery: electronic money and payment institutions are both mentioned in relation to corruption and bribery.

Conclusions: Evidence shows what e-money, specifically pre-paid cards, have been used by terrorist groups to finance their activities in the past. Given the low amounts of money used and the fast speed of transactions makes the detection of these transaction extremely challenging. However, cash is still a preferred way to send money to conflict zones or to avoid traceability. Law enforcement authorities 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 authorities 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 cumulated large flows of money it represents, especially when loaded onto prepaid cards or vouchers of value benefitting from customer due diligence exemptions, which can be used online or offline and can be purchased by cash. While some connection is often needed with e-money issuers' agents or distributors in their delivery channels there are cases where customer due diligence are not properly performed, in particular when cards are sold by distributors who are not obliged entities. Nevertheless, criminal organisations prefer until now 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 of low value that are not linked to a current account (cash-based products[76]) offer anonymity features similar to cash because they are exempt from customer due diligence measures. Particular concerns concerning prepaid cards are also linked to situations where there is no limit to the number of cards a customer could own. 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 of 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 may provide evidence of legitimate income and are not within the scope of sanctions regime. Regtech[77] solutions were also identified as key current risks, with increased risks of computer fraud and use of false documents.

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

[77] The term RegTech was first coined by the UK's Financial Conduct Authority(FCA) in 2015 who called it: "A subset of fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities." In simple terms it refers to any technology that ensures companies comply with their regulatory requirements.

In respect of TF, e-money products is of particular interest for moving safely money to conflict zones, including for terrorist financing purpose.

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 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 yet identified. 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 authorities; 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 AMLD, some e-money products benefit from an exemption regime which means that when some risk-mitigating conditions are met (the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 150, which can be used only in the Member State of issuance, the payment instrument is used exclusively to purchase goods or services and cannot be funded with anonymous electronic money), certain customer due diligence measures need not to be applied. On the other hand, the AML Directive require e-money issuers to always carry out sufficient monitoring of the transactions, the thresholds for allowing these customer due diligence derogations have already been lowered in 2018 and the European Commission envisages to possibly further limit these possibilities in the future.

In addition, Member States may require electronic money issuers whose head office is situated in another Member State (home Member State) but operating in their jurisdictions (host Member State) under either the right of establishment or the freedom to provide services to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the institution operating on a cross-border basis, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.

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 authorities 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 very 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. As a result of their supervisory activities, National competent authorities identified a relatively small number of breaches. In 2018, where breaches were identified, these were mostly serious, with egregious breaches identified in only few cases. In 2019, breaches identified were mostly minor or moderate, with no egregious breaches reported[78]. However, the main contributing factors that expose the sector to ML/TF risks are those associated with distribution channels. This is because the use of intermediaries in the distribution chain is common in the sector, which can make adequate AML/CFT controls and oversight more difficult.

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 assesses 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 AMLD, e-money products benefit from an exemption regime which means that when some risk-mitigating conditions are met (the payment instrument is not reloadable, or has a maximum monthly payment transactions limit of EUR 150, which can be used only in the Member State of issuance, the payment instrument is used exclusively to purchase goods or services and cannot be funded with anonymous electronic money),

[78] EBA report on money laundering and terrorism financing risks affecting the EU's financial sector, paragraph 106: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

certain customer due diligence measures need not to be applied. On the other hand, the AML Directive requires e-money issuers to always carry out sufficient monitoring of the transactions, the thresholds for allowing these customer due diligence derogations have already been lowered in 2018 and the European Commission envisages to possibly further limit these possibilities in the future.

In addition, Member States may require electronic money issuers whose head office is situated in another Member State (home Member State) but operating in their jurisdictions (host Member State) under either the right of establishment or the freedom to provide services to appoint a central contact point in their territory. That central contact point shall ensure, on behalf of the institution operating on a cross-border basis, compliance with AML/CFT rules and shall facilitate supervision by supervisors, including by providing supervisors with documents and information on request.

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, that may require additional staff in addition to technology, increasing 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 significant (level 3).

Risk level

As regards terrorist financing, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, money laundering and terrorist financing, is level 3, HIGH.

Mitigating measures

For the competent authorities:

- Member States competent authorities should carry out more robust risk assessment of the sector to the extent that Electronic money issuers are active on their territory, clearly identifying and assessing all ML/TF risk factors in their national risk assessments[79].

[79] For that purpose, national competent authorities can notably refer to EBA's Risk Factors Guidelines, Sectoral guideline number 10 for electronic money issuers (pages 77 to 83):

- Member States competent authorities should also consider how best they can use a mix of different supervisory tools to supervise the sector more efficiently and in line with that risk profile. While full-scope on-site inspections may not be necessary in every case, Member States competent authorities should consider how they can use, for instance, on-site thematic reviews to ensure adequate supervisory coverage of a sufficiently large number of firms.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

For the European Commission:

- The European Commission should reassess whether the current exemption contained in the AML directive with respect to customer due diligences in the context of electronic money transaction keeps a legitimacy and should be maintained or whether it could possibly be further limited.

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

8. Transfers of funds and money remittance

Product

Transfers of funds and money remittance

Sector

Credit and financial institutions — money value transfer services

General description of the sector and related product/activity concerned

Under 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), 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including (a) a credit transfer[80]; (b) a direct debit[81]; (c) a money remittance[82], whether national or cross border; (d) a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.

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 by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs, 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. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. They represent one of the most risky activity among the different payment services performing transfer of funds. 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.

Most migrants use MVTS services for a variety of reasons, including because they offer lower fees than banks, are more widely accessible (i.e. opening hours), and more fundamentally, because in most developing countries, the network on MVTS is the widest (as compared to banks) and many people do not have access to bank accounts in developing countries. According to the World Bank, inflows from remittances were equivalent to more than 10% of 2015 GDP in 29 countries, and more than 20% in eight of them[83].

[80] As defined in point (1) of Article 2 of Regulation (EU) No 260/2012.
[81] As defined in point (2) of Article 2 of Regulation (EU) No 260/2012.
[82] As defined in point (13) of Article 4 of Directive 2007/64/EC.
[83] http://www.worldbank.org/en/topic/migrationremittancesdiasporaissues/brief/migration-remittances-data

General ECB statistics also show that in 2019, the total amount of remittances sent from EU Member States amounted to EUR 200,4 billion, with a slight increase compared to 2018 (EUR 194,5 billion)[84].

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. Most licensed or registered MVTS providers hold accounts at banks in order to process transfers and settle accounts with agents both domestically and internationally. However, settlement may be done through wire transfers, often involving aggregated amounts, processed through the international banking system. In addition, settlement can be done through third party payment providers[85]:

- Proceeds of crime are laundered through settlement systems in a non-EU country. 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.

Rogue agents usually perform transactions using fake IDs and fake invoices.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to money value transfers services shows that terrorist groups recurrently use this method. Payment institutions, e-money institutions and bureaux de change are also perceived by several CAs as being particularly vulnerable to TF, in particular as regards the use of cash, pre-paid instruments, the importance of transactions from/to high-risk jurisdictions and

[84] https://sdw.ecb.europa.eu/quickview.do?SERIES_KEY=169.PSS.A.D0.F000.MRS.Z00Z.VT.X0.20.Z01.E
[85] FATF guidance for a risk-based approach for money value transfers services, 2016, page 9: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf

the anonymity allowed from transactions below the CDD threshold[86]. Law enforcement authorities 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 still considered as very significant (level 4).

Money laundering

Organised crime groups recurrently use this method. Law enforcement authorities 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.

From Europol Financial Intelligence Public Private Partnership (EFIPPP) information:

Related to live distance child abuse typology: the presence of reliable money remittance systems is an environmental factor that allows for this type of crime to emerge. In addition, the use of MVTS is mentioned as a possible indicator for non-delivery scams, counterfeit goods (money transfers to high risk jurisdictions), illegal wildlife trade and match fixing and betting.

Finally, in relation to ransomware and cryptocurrencies typologies, an indicator of ransomware payments is a payment to a crypto exchange platform or foreign-located Money Service Business (MSB)- such as Western Union, MoneyGram - in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for crypto exchange platform entities.

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).

[86] EBA Opinion on ML/TF risks, paragraph 20: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

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 authorities 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. A decline in the number of correspondent banking relationships is a source of concern for developing countries where remittance flows are a key source of funds for households as it has a significant impact on Remittance service providers' ability to access banking services[87].

b) risk awareness

According to the competent authorities, risk awareness in the sector is high (due to the recent terrorist attacks). Law enforcement authorities notice that the bigger players are more often misused by terrorists than the smaller ones due to their bigger agent networks in different countries. While MVTS providers have put in place measures to identify their customers and verify their identities, an effective ongoing monitoring of transactions would require a better access to relevant information, often held by law enforcement authorities, that would help them identify terrorist financing risks before they materialise. Likewise, law enforcement authorities' 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. However, it is important to highlight that the entire sector is not submitted to the same level of risk and must be addressed on a case-by-case basis. In that regard, the FATF interpretive note to recommendation 10 (Customer Due Diligence) sets out examples of potentially higher-risk situations, including businesses that are cash intensive, or involving non-resident customers.

c) legal framework and checks

Registered and authorised MVTS providers are subject to AML/CFT requirements at EU level. Regulation (EU) 2015/847 specifies the duties of payment service providers regarding the information on the payer and the payee that must be attached to the fund transfers. It also requires payment service providers to put in place effective procedures to detect transfers of funds that lack this information, and to determine whether to execute, reject or suspend such transfers of funds. Its aim is to prevent the abuse of fund transfers for ML/TF purposes, to detect such abuse should it occur, and to allow relevant

[87] FSB, Stocktake of remittance service providers' access to banking services, March 2018, page 7 https://www.fsb.org/wp-content/uploads/P160318-3.pdf

authorities promptly to access information on the payer and the payee associated with a particular transfer where necessary. The effectiveness of checks in place remains however until now rated as generally poor by supervisors. 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 authorities 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 authorities 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 very significant (level 4).

Money laundering

The MVTS sector is made up of a very diverse range of actors, from independent business with limited outlet locations to large multinational corporations having on the contrary a big geographical scope and using a network of agents. Money laundering vulnerability related to money value transfers services cannot be assessed without considering that most important MVTS providers rely on agents. Therefore agents constitute the main factor for risk exposure for MVTS providers.

a) risk exposure

MVTS services allow for speedy transactions. They are more and more provided by companies ensuring a fully traceable and digital service -and this change was accelerated by the COVID 19 pandemics. They remain however, in a number of cases, cash-based and. 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 linked to their high speed, the consolidated volume they represent (although individual transactions are usually low), factors that can be worsen in cases where they involve cash-intensive services 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 does not have 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 concerns also arise, first for the developing countries that rely on the income and the important weight they represent in their gross domestic product, and 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 de minimis thresholds are in place for triggering customer due diligence obligations, leading to possibly a too light oversight of agents in the context of a very competitive sector, pushing sometimes to 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 risk 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. Regulation (EU) 2015/847 specifies which information on the payer and the payee must accompany the fund transfers. It also requires payment service providers to put in place effective procedures to detect transfers of funds that lack this information, and to determine whether to execute, reject or suspend such transfers of funds. Its aim is to prevent the abuse of fund transfers for ML/TF purposes, to detect such abuse should it occur, and to allow relevant authorities promptly to access information on the payer and the payee associated with a particular transfer where necessary. Because of the reliance on agents, supervision of the sector is very challenging. Firms rely more and more on new technologies and software to conduct robust customer due diligence and agent oversight, measures which should enhance their efficiency once they will be more generally used. MVTS providers need to develop trainings of their agents to make them perform proper customer due diligence while they should more efficiently ban rogue agents from their networks.

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 among MVTS providers 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).

Risk level

As regards terrorist financing, the level of threat has been assessed as very significant (4), and the level of vulnerability has also been assessed as very significant (4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant (3).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
➔	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for money laundering is level 3, HIGH and for terrorist financing level 4, VERY HIGH.

Mitigating measures

For the competent authorities:

- Member States could envisage lowering or eliminating thresholds to occasional transactions, consider applying systematic 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.
- Considering the cross-border nature of ML/TF, Member States should encourage relevant authorities in charge of preventing and combatting ML/TF to request support from Europol.

For the sector:

- Payment service providers must take measures to detect missing or incomplete information on the payer or the payee in a transfer of funds, and procedures in place to manage a transfer of funds lacking the required information.

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 European Commission:

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

9. 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.

The terminology of "Hawala" is less used currently in the investigative environment. **Money laundering controller networks** (MLCN) or international money laundering networks are the "successors" of the hawaladars.

Members of diaspora and migrant communities use these MLCN 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 MLCN 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 value (cryptocurrency, gold, goods, etc.) 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 and tax 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 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.

Margins on even small international transfers may be as low as 1%, far less than banks' charges. It is not only cheaper to use a *hawala* merchant than a bank, but quicker and easier too. Transfers can typically be picked up the same day. Customers do not need to prove their identity, or explain why the money is being sent. That is why it is essential in countries, where large parts of the population do not have identity documents.

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; transformation of the value into cryptocurrencies or gold; 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).

The impact of COVID-19

COVID-19 has affected and still is affecting hawala negatively, having dried up cross-border trade and closed the small shops and businesses that do transfers. But the bigger hit has been to goods trade. With borders closed, importers did not need to move money around, or to borrow to cover liquidity gaps[88]. In countries like Somalia, where telecoms operators are largely unregulated, hawaladars have started to work as mobile-money agents on the side and transactions around the country can be done instantaneously on phones. According to the World Bank, around three-quarters of Somalis use mobile money—mostly denominated in dollars—and it is more common than cash[89].

On the other hand, LEAs inform that the post-lockdown time has been one of the busiest periods for the money launderers globally, as they saw a huge opportunity to pump unaccounted money into the market by financing small-time traders and people who were looking for funds to start a trade of their own[90].

Threat[91]

The scale of hawala in the EU is unknown. As a tool for comparison, the central bank of the UEMOA (West African Economic and Monetary Union) space of eight countries says that over $450 million is moved back and forth each year through this method[92], with the actual figure possibly being at least twice or thrice the initial estimate. Estimations in South Asia refer to nearly $400 billion passing through the hawala networks every year[93]. Europol is also aware of several multi-million EUR on-going money laundering investigations focusing on criminal hawala[94] in Europe.

Hawala is known to be associated with certain businesses of certain ethnic communities (India, Afghanistan, Pakistan, Iran, United Arab Emirates, sub-Saharan Africa, Somalia and China) that are common in the EU. Examples of the kinds of business involved are travel agencies, pawn shops, mobile

[88] https://economictimes.indiatimes.com/news/economy/foreign-trade/importers-of-chinese-goods-face-supply-constraints-unable-to-pay-via-hawala-routes/articleshow/74143982.cms?from=mdr

[89] World Bank Group, *Somalia Economic Update*, August 2018: https://documents1.worldbank.org/curated/en/975231536256355812/pdf/REPLACEMENT-PUBLIC-Somalia-Economic-Update-3-FINAL.pdf

[90] Thus, for instance in Africa: https://qz.com/africa/2086170/the-rise-of-informal-money-transfers-in-west-africa/

[91] For a thorough general description, see Bunt, Henk van de, "The Role of Hawala Bankers in the Transfer of Proceeds from Organised Crime", in Siegel, D. and Nelen, H. (editors), *Organized Crime: Culture, Markets and Policies*; Springer, 2008.

[92] Synthèse des résultats des enquêtes sur les envois de fonds des travailleurs migrants dans les pays de l'UEMOA, BCAO, 2013 : https://www.bceao.int/sites/default/files/2017-12/synthese_des_resultats_des_enquetes_sur_les_envois_de_fonds_des_travailleurs_migrants_dans_les_pays_de_l_uemoa.pdf

[93] Estimate by late Dr Roger Ballard, hawala expert and director of the University of Manchester's Centre for Applied South Asian Studies (CASAS).

[94] Council of the European Union, "The role of criminal "Hawala" and other similar service providers (HOSSPs) in illegal immigration, money laundering and terrorism financing – recommendations for changes and other initiatives"; Brussels, 2017.

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.

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[95] 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.).

From Europol Financial Information Public Private Partnership (EFIPPP) typology information:

The use of Alternative Banking Platforms is identified in relation to match fixing/betting. EFIPPP also confirms the use of Hawala as one of the money laundering tools for money laundering controller networks. They use net settlement, i.e. no funds transferred for each and every transaction, using a cash pool to pay the beneficiary. They could be therefore described as the successors of the hawaladars (cash-in and cash-out). In relation to Trade-Based Money Laundering (TBML): Money/cash is not directly transferred but transformed into other value (cash, gold, goods, cryptocurrencies, etc.). By means of TBML, such as import/ export of goods and Informal Value Transfer Systems (IVTS), the network transfers funds or an equivalent value payable to a third party in another geographical location.

It has been reported that at least some individuals subject to sanctions against Russia ('oligarchs') may have anticipated sanctions even months before the war of aggression against Ukraine and moved their money through Hawala to escape them[96].

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). This cooperation may take place in the framework of national risk assessments, the organisation of conferences with private sector engagement, or FIUs informing the financial sector on emerging threats and the financial sector issuing suspicious transaction reports as a result.
- Carry out administrative inspections 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. The points where those networks are more vulnerable being:
    - Cash handovers.
    - Cash transportation.

[95] Nevertheless, while it is not always possible to follow the money, the value along the transformation scheme can still be followed.
[96] As published by Business Insider: https://www.businessinsider.com/russian-oligarchs-sanctions-movement-money-hawala-ukraine-war-2022-4?r=US&IR=T

    - International transactions made by third parties.
    - Money Service Businesses, Exchange Houses and Hawaladars in the cash pool.
    - OTC Crypto Brokers.
    - Tax and customs declarations.
- In the most affected countries, establish specialised investigation teams within the anti-money laundering or drugs units, as the work against criminal hawaladars often involves developing physical and technical surveillance on the suspects involved in cash movements related to drug traffics.
- Set up actions in airports and ports focusing on cash couriers.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

10. 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 ('PSD2')[97]. They are listed in Annex I of PSD2 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;
- issuance of payment instruments;
- payment transactions acquisition.

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 wake of the digitalisation of services. These services are referred to as payment initiation services and account information services. The money laundering and terrorist financing risk of these operations is considered the most relevant in the context of this fiche. Other specific aspects are dealt with in other parts of the Supra-national risk assessment[98].

Payment initiation services allow consumers to pay for their purchases by a credit transfer instead of a card payment. The payment initiation service provider can receive information whether 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 this basis, the web merchant may decide to ship the goods or provide 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.

Most of the PSD2 became applicable on 13 January 2018, some selected provisions on strong customer authentication (SCA) and access to payment accounts on 14 September 2019. PSD2 does not regulate all payments. Payments in cash or paper cheque payments are not covered. Payment transactions by a provider of electronic communication networks, under a certain value are also excluded from the scope of the Directive.

In 2021, the Commission consulted stakeholders on remaining obstacles as well as possible enabling actions that could be taken to ensure a wide availability and use of instant payments in the EU. Instant

[97] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 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 (Text with EEA relevance); *OJ L 337, 23.12.2015, p. 35–127.*

[98] See the specific fiches on *Hawala* or crypto-assets.

payment represent an innovation opportunity but will also raise new challenges that will be carefully considered to ensure that the money laundering and terrorism financing risks are mitigated appropriately.

The total value of payment transactions in the EU involving non-monetary financial institutions reached EUR 195,1 trillion[99] in 2019. The large majority of payments was done electronically. The total number of payment transactions in the euro area increased by 8.1% to 98.0 billion in 2019 compared with the previous year, with a total value of EUR 162.1 trillion[100]. Card payments accounted for 48% of the total number of non-cash payments in the euro area[101].

The number of cards in the euro area with a payment function increased in 2020 by 6.5% to 609.3 million. With a total euro area population of 343 million, this represented around 1.8 payment cards per euro area inhabitant[102].

SEPA

The Single Euro 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 around 465 million people in the 27 EU Member States and other non-EU countries (United Kingdom, Iceland, Norway, Liechtenstein, Switzerland, Monaco, San Marino, Andorra and Vatican City State/Holy See)[103].

Retail payment systems

Retail payment systems in the EU are payments made by the public, with a relatively low value, a high volume and limited time-criticality. In 2019, around 44 retail payment systems existed in the EU as a whole[104] and almost 45 billion transactions were processed by retail payment systems in the euro area worth EUR 35.0 trillion[105].

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.

In 2019, there were 9 active large value payment systems[106] in the EU. The two main large-value payment systems in the euro area (TARGET2 and EURO1/STEP1) settled 141,5 million transactions amounting to EUR 497 trillion in 2019[107].

Payment service providers

Banks are players in national and international payment systems. Some 120 billion cashless payments were made by non-bank payment service providers (the nonfinancial sector **and** non-monetary financial

[99] ECB Payment statistics report.
[100] https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-retail-payments-factsheet_en.pdf
[101] https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-retail-payments-factsheet_en.pdf
[102] ECB, Payments statistics: 2020, 23 July 2021: https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2020~5d0ea9dfa5.en.html
[103] https://www.europeanpaymentscouncil.eu/about-sepa
[104] https://sdw.ecb.europa.eu/reports.do?node=1000002752
[105] https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/200924-retail-payments-factsheet_en.pdf
[106] https://sdw.ecb.europa.eu/reports.do?node=1000002752
[107] https://sdw.ecb.europa.eu/reports.do?node=1000001963

institutions[108]) in 2019 at EU-27 level[109]. More than half (62 billion) of those were card payments, while credit transfers or direct debits represented respectively 30 billion and 22 billion payments[110].

Within the EU, not only credit institutions are allowed to provide payment services.

These can also be provided by payment institutions, e-money institutions, post giro institutions and regional or local authorities where they do not act as public authorities. Payment institutions emerged with the adoption of the Payment Service Directive. These companies can provide payment services and engage in other business activities; they are not allowed to take deposits or issue e-money. Under PSD2, new categories of payment service providers were introduced: payment initiation service providers and account information service providers. These actors can provide exclusively the services of payment initiation and account information respectively.

Even though the introduction of payment institutions has increased competition in the payments market, the majority of provided payment service are still performed by credit institutions.

As for the other players, EU-wide there were[111]:

- 682 authorised payment institutions;
- 1640 exempted payment institutions according to article 32 of PSD2;
- 239 e-money institutions and
- 1331 Service providers excluded from the scope of PSD2' under points (i) and (ii) of point (k) and point (l) of Article 3 of PSD2 .

The distribution of payment institutions (authorised payment institutions and small payment institutions) is distributed among countries in the EEA. The biggest countries account for the largest numbers of payment service providers: Germany (11%), Netherlands (10%), France (9%), Spain (8%), and Sweden (7%), Italy (6%), account for 51% of all authorised payment institutions in the EEA. As for the exempted payment institutions, it is worth noticing that 85% were registered in Poland[112]

More general data on the number of financial institutions providing payment services in the EU can be found in the central registers of the EBA.

Description of the risk scenario

Perpetrators are using the banking and financial system to channel their funds through bank accounts, credit transfers and direct debits, peer-to-peer transfers made with a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics.

Effects of the Covid-19 pandemic: Misuse public funds

Criminal actors use a variety of techniques to exploit vulnerabilities in processes relating to the application and distribution of public funds. However, a common approach is the rapid movement of funds out of the jurisdiction by quickly withdrawing the funds in cash once government agencies transfer the financial aid.

[108] Non-monetary financial institutions comprise: Financial vehicle corporations, Euro area financial corporations engaged in lending, Investment funds other than money market funds (non-MMF investment funds), Insurance corporations, Pension funds, Lists of financial institutions: https://www.ecb.europa.eu/stats/financial_corporations/html/index.en.html
[109] See table 6: Number of payment transactions involving non-MFIs.
[110] Based on table 6 as well as 7.1 & 7.2 of ECB Payment statistics report 2020.
[111] https://euclid.eba.europa.eu/register/pir/search
[112] https://euclid.eba.europa.eu/register/pir/search

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.

Most 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 authorities cannot track the originator or beneficiary of the transaction in such cases. The misuse of payment services requires specific skills but, according to law enforcement authorities, these skills are commonly widespread within terrorist groups and do not constitute an obstacle (mobile/internet payments are quite easy). The individual average amounts of the payments concerned appear to remain, nevertheless, quite limited,.

Conclusions: terrorist groups are making use of 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. While the overall amount they represent may be significant, the individual average amounts of the payments concerned remain nevertheless 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 the use of funds deposited on account: a customer might not be submitted to customer due diligence checks, if the payment or transfer of funds is below the threshold triggering compulsory checks and does not raise particular_suspicion of money laundering or terrorist financing. This risk scenario concerns both the moments of 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[113]. It requires some planning and knowledge of how the banking systems work.

According to law enforcement authorities, payment services providers (PSPs) can be used for criminal purpose, notably by money mules. For example, a PSP has been investigated by several EU Member States. The PSP registered in one EU Member State also 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 payment cards (as the PSP is a Visa and Mastercard card issuer). The cards were taken out of Europe and cash was withdrawn in Colombia.

In addition, the Europol Financial Intelligence Public Private Partnership (EFIPPP) identifies multiple ways of criminal use of payment services:

- Use of credit cards, e-money and payment institutions as financial products/institutions in relation to corruption and bribery.
- A transactional indicator of ransomware payments is the payment to a crypto exchange platform or foreign-located Money Service Business (MSB) – such as Western Union, MoneyGram – in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for crypto exchange platform entities.
- Ransomware criminals ask their victims to pay a ransom through online payment method, typically cryptocurrency, to regain control of their data. Hackers typically demand ransoms in cryptocurrency.

A victim indicator for investment fraud: Increasing online presence and use of online payment services of potential victims, especially among vulnerable segments of the population, such as the elderly or those on lower incomes.

Example of a company involved in the illegal sale of football tickets and money laundering, using Third Party Providers: Company A was incorporated in Spain. It was reselling and touting football tickets in the UK, which is illegal in the UK and thus a predicate offence for money laundering. Company A has an account in Bank X located in Spain. Company A worked together with a Third Party Payment Processor (TPPP) registered in Germany which maintains business account in Bank Y in UK. TPPP's task is to support merchants like Company A at the point of sale regarding payment processes and sales channels. Following many requests for ticket refunds due to COVID-19 pandemic, Company A transferred 175,000 pounds to the TPPP's account in Bank Y to remedy its negative account balance. The funds are transferred to another UK banks which then distributed the refunded amounts to the ticket holders.

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. The key emerging risks identified by National Competent Authorities include the cash-intensive nature of the services offered, the prevalence of occasional transactions rather than established business relationships, the involvement of high-risk jurisdictions payment institutions, the large volume and high speed of transactions, the use of new technologies to facilitate the onboarding of customers remotely and the distribution channels used. In this context, the level of the money laundering threat related to payment services is considered as significant (level 3).

Vulnerability

Terrorist financing

When assessing the terrorist financing vulnerability related to payment services, one must take into account their cash-intensive nature, the prevalence of occasional transactions on established business relationships, the large volume and high speed of transactions, the possible involvement of high-risk jurisdictions in which PIs operate, the use of new technologies to facilitate the onboarding of customers remotely and the distribution channel used.

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 (when 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

While the sector has put in place guidance to detect the relevant red flags on terrorist financing, the risk awareness remains perfectible. While Competent authorities noted a good level of reporting, and an improvement in the level of controls in place in the sector, a large proportion of these controls are still rated as poor or very poor. Despite a significant risk profile and although almost all Competent authorities indicated they carried out some supervisory activity during the period under review, the EBA notes that the sector, in view of its risk profile, saw a relatively low level of supervisory activity[114]. Competent authorities are 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 not to be yet fully efficient. As far as the legal framework is concerned, it covers equally credit institutions and other payment service providers, such as payment institutions and e-money 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, credit and payment institutions do not have access to relevant intelligence, often held by law enforcement authorities, that would help them to better identify and prevent terrorist financing risks before they materialise. Likewise, law enforcement authorities 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). While the level of controls in place in this sector has progressed, a large proportion of these controls are still rated as poor or very poor and the level of awareness of the risk vulnerability must improve. The legal framework and checks are the basis of a good level of reporting. The sector has a relatively low level of supervisory activity and there is also high residual risk 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).

[114] EBA Opinion on ML/TF risks, paragraph 53: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

Money laundering

When assessing the money laundering vulnerability related to retail payment services, one must take into account their cash-intensive nature, the prevalence of occasional transactions on established business relationships, the large volume and high speed of transactions, the possible involvement of high-risk jurisdictions in which PIs operate, the use of new technologies to facilitate the onboarding of customers remotely and the distribution channel used.

a) risk exposure

Risk exposure is inherently high due to the characteristics of payment services, which involve very significant volumes of funds, and are associated with a broad diversity of customers and jurisdictions, including high risk ones. Although payments are generally not anonymous (when they are linked to an identified account), they are often not monitored (notably if they are under the amount requiring systematic customer due diligence measures for occasional transactions and take place outside of a business relationship framework) and may entail contact with higher risk customers or countries, especially where cross-border movements of funds are involved. Payment institutions often use agents to process payments, which significantly increases the risk due to the risk that these agents may collude with criminals[115]. They also make use of new payment methods, which may also 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 crypto-assets/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 remains high and risk awareness has not yet brought sufficient efficiency in monitoring the payment services. 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).

[115] EBA Opinion on ML/TF risks, paragraph 53: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

Risk level

As regards **terrorist financing**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (level 3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (level 3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, terrorist financing and money laundering is HIGH.

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;
- promote cooperation between law enforcement agencies and financial institutions in order to improve effectiveness of terrorist financing alert systems at supranational level;
- submit exchange of crypto-asset to funds and of funds to crypto-assets activities to AML/CFT obligations;
- consider possible lowering of the thresholds triggering compulsory customer due diligences for occasional transactions involving funds.

For Member States / competent authorities:

- Member States should ensure that supervisors conduct regularly on-site thematic inspections focusing on risk assessments of payment services providers, and ensure that their alert systems are effective.
- In addition, competent authorities should continue to raise risk awareness and risk indicators relating to terrorist financing with payment service providers (PSP), via close Public Private Partnership cooperation.
- Member States could envisage lowering or eliminating thresholds for occasional transactions, applying customer due diligence to all transactions so that payment institutions efficiently monitor and detect suspicious transactions.
- Considering the cross-border nature of ML/TF, Member States should seek international cooperation encourage relevant authorities in charge of preventing and combatting ML/TF to request support from agencies such as Europol.

11. Crypto assets and Virtual currencies

Product

Crypto-assets, including so-called virtual currencies

Sector

Crypto-assets issuers and service providers

Description of the risk scenario

According to its opinion on ML/TF risks released in March 2021[116], the EBA notes that compared to its previous Opinion issued in 2019, risks arising from crypto-assets appear to have increased further. They attribute this to the growth of the crypto-asset market, in terms of both the number of transactions processed and customers, the increased range of products and services and their often-unregulated nature o and associated lack of customer due diligence measures[117], and a compliance immaturity and overall limited overall understanding of ML/TF risks in the sector. The main factors contributing to the increased exposure to the ML/TF risks is said to be the limited transparency of crypto-assets transactions and the identities of the individuals involved in these transactions. We note, however, that crypto-assets transactions conducted on public distributed ledgers leave immutable traces and are there for everyone to see. Persons engaging in ML/TF via such crypto asset transactions expose themselves to public scrutiny of their transactions[118].

Custodian wallet providers and providers engaged in exchange services between virtual and fiat currencies are now within the scope of the AML/CFT legal framework by defining them as obliged entities in the AMLD. The related provisions apply and should now have been transposed by all Member States in January 2020. However, not all MS have transposed these provisions yet[119]. The European Commission's proposal for a Regulation on Markets in Crypto-assets[120] (MiCA) published in September 2020 will have, when adopted, the effect of expanding the EU financial services regulatory perimeter to a wide range of crypto-asset activities. With the EU's proposals released in July 2021 to strengthen the EU's AML/CFT framework, AML rules will be extended to all crypto-asset service providers covered by MiCA. This will also align EU AML/CFT rules with the latest international standards and guidance from the FATF.

However, a particular attention will still have to be given on how to best address possible emerging threats having a link with the crypto-assets and their industry but not fitting fully with existing legal framework in that field. This is in particular the case of **non-fungible tokens (NFTs),** assets representing a unique token that acts as a non-duplicable digital certificate of ownership for a specific digital asset, and which legal qualification may differ from a jurisdiction to another. First analysis by

[116] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

[117] EBA report on crypto-assets, January 2019.

[118] To a certain degree. While it is true that transactions are recorded in the blockchain, it does not automatically mean that these persons can be identified. Also, there are numerous privacy coins that leave almost no traces in their respective blockchain.

[119] 5th Anti-money laundering directive – transposition status (last updated in April 2022).

[120] Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.

regulators suggest that NFTs should not always be considered as crypto-assets[121], especially if they are not used as payment or instruments for investment. Exposure to ML risks arise due to the limited application of customer due diligence checks on many of the major NFT sales platforms and the fact that many services seem now created for the express purpose of obfuscating the origin and destination of funds through NFTs. It is possible for criminals to set up an account, list a number of NFTs and then purchase said NFTs from themselves for an inflated price. The current popularity experienced by NFTs, and subsequent high prices, further complicate the process of identifying which transactions are wash trading and which are legitimate purchases. There are, meaning that the proceeds from malicious sales can be hidden with relative ease.

Another key concern also arise from **crypto-assets exchange, lending or transfer services,** activities normally offered by regulated crypto-assets services providers but made through decentralized or distributed application, often run on a decentralized ledger, with no legal or natural person with control or influence over it, often referred to as 'decentralised finance' (DeFi)[122]. There seems to be a broadly shared consensus among jurisdictions that DeFi applications should not be considered crypto-assets services providers if there is no identified body that can be held liable for their use.

This makes DeFi's exposure to risk of ML/TF rather high, as DeFi applications can be used to avoid existing AML/CFT legislation and the "travel rule" obligations as set out by the FATF[123]. However, in case a person or a managing body can be identified, despite its qualification, the DeFi application shall be treated as a crypto-assets services provider and fall under the same AML/CFT obligations. Therefore, much like with NFTs, DEFIs may be subjected to the application of the relevant rules covering crypto-assets on a case-by-case basis but keep posing regulatory challenges that are not yet fully addressed and could conduct to take additional measures to better tackle them in the future.

Threat

Crypto-assets 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 crypto-assets. Several law enforcement authorities indicated that ML/TF risks from crypto-assets have increased further since 2019[124], linked to the growth of the crypto-asset market, in terms of transactions processed and number of firms' clients that use crypto-assets or are crypto-assets service providers. Law enforcement authorities identify the limited transparency of transactions and identities of end-customers involved in crypto-asset activities as the most significant risk factor that may facilitate illegal activities such as fraud, trading of illicit goods/services and terrorist financing.

Europol regards Bitcoin as the crypto-assets of choice for the majority of criminals, but anticipates a more pronounced shift towards anonymity-enhanced crypto-assets, which offer greater anonymity and capacity to obfuscate transactions. Some of such anonymity enhanced crypto-assets are, however, harder to acquire and transact than Bitcoin.

Exchangers can offer crypto-assets to crypto-assets transactions that obfuscate the transaction trail and decentralised mixers have also been used.

[121] See the FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, page 24, paragraph 53:
https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf October 2021.
[122] Ibid, page 27, paragraph 67.
[123] Ibid, page 56, paragraphs 178-180.
[124] EBA report on money laundering and terrorism financing risks affecting the EU's financial sector, figure 1 page 13:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf , March 2021

A particular set of challenges arises from crypto-assets services provided by criminals or non-compliant entities:

- individuals buy/sell large volumes of crypto-assets for any asset peer-to-peer (no intermediation) without involvement of registered crypto-asset service providers subject to AML/TF requirements; and
- payment services providers offering crypto cards[125] were initially offered only for Bitcoin, but there has been a shift towards support of multiple crypto-assets. They often register in jurisdictions with 'favourable' regulatory arrangements that do not facilitate their monitoring.

Law enforcement agencies also face particular challenges in collecting information when crypto-assets services are offered in a country other than that in which the originator / beneficiary are located (which itself may be anywhere in the world).

Europol Financial Intelligence Public Private Partnership (EFIPPP) information from typologies

Match-fixing/betting: Virtual assets are used to open betting accounts online.

Corruption and bribery: Virtual assets transactions are financial products used in relation to corruption and bribery, and Virtual Assets Service Providers are used.

Ransomware and cryptocurrencies.

ML and cryptocurrency.

ML Controller Networks (MLCNs): the services of MLCNs include cash out (cash is collected in a jurisdiction and cash is delivered in any other jurisdiction), cash swap (cash is collected in a currency and paid out in another currency, including cryptocurrency) and account payment (the broker collects the cash and makes a payment on behalf of the client through a compensation scheme to balance and move value).

A technique used is Trade Based ML (TBML). Money/cash is not directly transferred but transformed into other value (cash, gold, goods, cryptocurrencies, etc.). By means of TBML, such as import/ export of goods and Informal Value Transfer Systems (IVTS), the network transfers funds or an equivalent value payable to a third party in another geographical location.

EFIPPP information from typologies:

Typology observed where ***child sexual exploitation (CSE)*** sites offer member subscription by paying in cryptocurrencies / virtual assets (usually in Bitcoins).

The CSE site will provide several addresses to pay a small amount in cryptocurrencies / virtual assets. These addresses can be traced to a main pooling address where the suspect(s) gather their funds. This trail can potentially be followed to a regulated crypto/virtual asset exchanger and the suspect thus identified.

Furthermore, it is possible to trace the payments to these clusters back to an exchange, identify buyers and discover additional links. Since the Blockchain record is permanent it is possible to continuously over time gather more evidence and find more subjects related to the purchase and distribution of CSE.

[125] A crypto credit card is a rewards credit card that offers cryptocurrency rewards on purchases instead of cash back or points. They function the same way as a normal credit card. This kind of cards can be used, for example, to circumvent CDD/KYC through direct cash deposits through crypto ATMs.

Investment fraud:

- Scammers take advantage of the recent decline in asset prices to sell fraudulent investments in gold, silver and other commodities labelled as a safe haven as well as low value stocks or high risk financial products such as derivative instruments and cryptocurrencies.
- Buy low, sell high schemes targeting commodities and real estate, cryptocurrencies or complex derivative products.
- A victim indicator is payments related to cryptocurrencies, derivative instruments (gold, shares, indexes and forex) and shares issued by companies with low capitalization (aka Microcap / "penny stocks") trading in the over-the-counter securities market.
- Transfers to cryptocurrency exchanges or to accounts in high risk jurisdictions.
- Very few or same bitcoin/crypto currency addresses used to collect payments from multiple victims.

Misuse of Public Funds:

- There is a range of different profiles of criminal actors who exploit the weaknesses of the system to accept, assess and process fiscal stimulus measures. A common feature of the fraudsters is that they have proficient IT skills to create sophisticated fake websites, to execute phishing attacks, to browse the Darkweb and deal with different anonymous cryptocurrencies.
- Transfers to cryptocurrency exchanges

Non-delivery scam: The merchant requests payments that are unusual for the type of transaction in question or unusual for the industry's pattern of behaviour. For example, instead of a credit card payment, the merchant requires a pre-paid card, the use of a money services business, convertible virtual currency, or that the buyer send funds via an electronic funds transfer to a high-risk jurisdiction

Counterfeit goods: Unusual payment methods, e.g. pre-paid cards, virtual assets, or via money services

Counterfeit goods: Financial products being used are a) E-Money and payment accounts (incl. virtual IBANs), b) Credit cards, c) Bank accounts (incl. virtual IBANs), d) Virtual assets. VASPs are among the financial institutions used.

Illegal trade: related to illegal wildlife trade, an indicator is deposits from money service businesses or crypto-currency exchanges.

Terrorist financing

Crypto-assets generally involve non-face-to-face customer relationships and may allow for anonymous – and not yet always traceable - 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. The assessment shows that terrorist groups may have an interest in using crypto-assets to finance terrorist activities. A limited, but growing number of cases related to crypto-assets have been reported[126]. The Egmont Group of FIUs has detected cases of terrorist groups using crypto-assets and groups are known to have given instructions on the internet (including via Twitter) on how to use crypto-assets.

Conclusions: Law enforcement agencies have information according to which terrorist groups may be using virtual currencies to finance terrorist activities. The global reach, the speed at which transactions can be carried out and the possible anonymity offered by their transfer, make

[126] 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.

crypto-assets particularly attractive for criminals seeking to carry out illicit transfers across jurisdictions and to operate beyond national borders.

Consequently, the terrorist financing threat related to virtual currencies is considered very significant (level 4).

Money laundering

Crypto-assets carry a significant ML/TF risk, due to the ease of transferring crypto-assets to different countries as well as the absence of homogeneous controls and prevention measures implemented at the global level, due to some delay by several jurisdictions in implementing FATF standards on virtual assets. Perpetrators use crypto-assets systems to transfer value or purchase goods anonymously (cash funding or third-party funding through virtual exchanges). The assessment of the money laundering threat related to crypto-assets shows that organised crime organisations may use them to access 'clean cash' (paying in and paying out). Not only cybercriminals use crypto-assets – other organised crime groups such as drug traffickers use them to move and launder the proceeds of crime. Crypto-assets 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: investigations show that criminal organisations' (not only cybercriminals') use virtual currencies and virtual assets. Consequently, the level of money laundering threat related to virtual currencies is considered very significant (level 4).

Vulnerability

Terrorist financing

In assessing the terrorist financing vulnerability related to crypto-assets providers, we must bear in mind that, while the EU started to regulate the provision of services involving crypto-assets in 2018 and is implementing further changes (the proposals for MiCA and the new AML/CFT package), the risks of crypto-assets being misused to finance terrorism are only just emerging.

a) risk exposure

When used anonymously, crypto-assets 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 easily identified, even if the transactions leave digital footprints that can be analysed. The implementation of FATF standards on virtual assets require crypto-assets 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) and to comply with AML/TF requirements, notably information duties on the originators and beneficiaries of crypto-assets transfers. This will reduce the scope for anonymous transactions with crypto-assets through crypto asset service providers.

b) risk awareness

This component of terrorist financing vulnerability is difficult to assess in a comprehensive manner but competent authorities and financial intelligence units have noted in their contacts with the crypto-assets services providers 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.

Crypto-assets are among the 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 crypto-assets where they act as intermediaries or exchange platforms between crypto-assets and fiat currencies (in the absence of a proper risk assessment); and

The sector is not yet well structured and the policies to increase the level of awareness were until recently rather limited.

c) legal framework and checks

AMLD5 introduced a first EU definition of virtual currencies 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. While related provisions should have been transposed by all Member States in January 2020, it is not fully the case yet[127].

The European Commission's proposal for a Regulation on Markets in Crypto-assets[128] (MiCA) published in September 2020 will have, when adopted, the effect of expanding the EU regulatory perimeter to a wide range of crypto-asset activities. The publication of the EU's proposals to strengthen the EU's AML/CFT framework in July 2021, include a proposal to align the scope of the AMLD with the activities covered by MiCA and to introduce an obligation for all crypto-assets services providers involved in crypto-assets transfers to collect and make accessible data concerning the originators and beneficiaries of the transfers of virtual or crypto assets they operate (the "travel rule" of the FATF). These proposals also imply to ban the possibility to use or open an anonymous crypto-assets account and to broaden to crypto-assets services providers the possibility to appoint contact points in Member States where they are active via freedom to provide services (as it is currently the case for Electronic money issuers and payment service providers).

These new rules, if adopted, will significantly enhance the monitoring of crypto-assets service providers, and ensure compliance with the relevant measures called for in the FATF Recommendations.

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 has significantly improved the monitoring of the virtual assets industry 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 supplemented with the legislative proposals of the EC to regulate the crypto-assets industry and its professionals stakeholder, in line with international standards. The inherent risk exposure remains high due to the characteristics of virtual assets and virtual currencies (internet-based, cross-border and anonymous). Nevertheless, the sector is getting more organised and has recently received a very comprehensive guidance and information on how to implement AML/CFT requirements[129].

Still, the level of terrorist financing vulnerability related to virtual currencies is considered very significant (level 4).

[127] 5th Anti-money laundering directive – transposition status (last updated in April 2022).
[128] Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final.
[129] See FATF updated guidance: https://www.fatf-gafi.org/documents/documents/guidance-rba-virtual-currencies.html

Money laundering

Crypto-assets are partially regulated in the EU and there is growing evidence of crypto-assets being misused for money laundering as well as a means of payment for prohibited goods such as drugs.

a) risk exposure

As mentioned above, when used anonymously, crypto-assets 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[130]) that cannot be identified. At the stage of the conversion, the use of cash also becomes a new element of vulnerability. The AMLD5 rules address this risks for 'providers engaged in exchange services between virtual currencies and fiat currencies'. However, several types of crypto-assets activities still fall today outside of the scope of Union legislation on financial services and the information obligations linked to transfers of virtual assets are not yet fully in place at EU level.

b) risk awareness

Crypto-assets rely on, in part, still recent technology but the level of risk awareness in the sector has significantly improved recently. The FATF international standards and their progressive implementation at EU level are responding to the need expressed by the sector for a clearer and more structured legal framework in which crypto-assets activities are subject to AML/CFT requirements.

Some specific risks are however linked to the absence of awareness of new high-value crypto-assets (such as some Non Fungible Tokens which can be considered as works of art). Another risk is linked to the possible control of some crypto-assets service providers by criminal organisation (either taken over by organised crime groups, or because the Virtual Asset Service Provider was created by an OCG).

c) legal framework and checks

Directive (EU) 2018/843[131] was the first legal instrument to address the risks of money laundering and terrorist financing posed by crypto-assets in the Union. It extended the scope of the AML/CFT framework to two types of crypto-assets services providers: providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers. Due to rapid technological developments and the advancement in FATF standards, it was then deemed necessary to review this approach.

The European Commission's proposal for a Regulation on Markets in Crypto-assets (MiCA) published in September 2020 will have, once adopted, the effect of expanding the EU regulatory perimeter to a wide range of crypto-asset activities. Further action is expected in 2021 with the publication of the EU's proposals to strengthen the EU's AML/CFT framework, including a proposal to align the scope of the AMLD with the activities covered by MiCA.

A first step to complete and update the Union legal framework will be achieved with the adoption of the MiCA Regulation[132], which set requirements for issuers of crypto-assets in the Union and crypto-asset service providers wishing to apply for an authorisation to provide their services in the single market. It also introduced a definition of crypto-assets and crypto-assets services providers encompassing a broad range of activities that corresponds to the FATF standards requirements and go even beyond:

[130] A dark net or darknet is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization, and often uses a unique customized communication protocol.
[131] 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; *OJ L 156, 19.6.2018, p. 43.*
[132] Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final.

- the custody and administration of crypto-assets on behalf of third parties;
- the operation of a trading platform for crypto-assets;
- the exchange of crypto-assets for funds;
- the exchange of crypto-assets for other crypto-assets;
- the execution of orders for crypto-assets on behalf of third parties;
- the placing of crypto-assets;
- the reception and transmission of orders for crypto-assets on behalf of third parties
- providing advice on crypto-assets;
- providing portfolio management on crypto-assets.

The MiCA regulation also introduce requirements for these services providers to be licensed and submit their senior management to fit and proper tests.

The Commission proposals of July 2021 to strengthen the EU's AML/CFT framework will allow to cover a greater scope of crypto-assets activities, by aligning the scope of the AMLD with all crypto-asset service providers covered by MICA in line with the FATF standards requirements. These proposals shall introduce an obligation for all crypto-assets services providers involved in crypto-assets transfers to collect and make accessible data concerning the originators and beneficiaries of the transfers of virtual or crypto assets they operate (thus applying the so-called "travel rule" contained in FATF Recommendation 15 on VASPs). They may also end the possibility to use or open an anonymous crypto-assets account and to broaden the possibility for Member States to require that crypto-assets services providers established on their with a head office situated in another Member State to appoint a central contact point (as it is currently already the case the case for Electronic money issuers and payment service providers).

These new rules, if adopted, will significantly enhance the monitoring of crypto-assets service providers, and ensure compliance with the relevant measures called for in the FATF Recommendations.

Conclusions: AMLD rules have significantly enhanced the monitoring of risks linked to virtual asset service providers, but it remains partially implemented and does not cover yet all virtual asset service providers. The EC AML legislative proposals released in 2021 will lead to strengthen the EU's AML/CFT framework, including a proposal to align the scope of the AMLD with the activities covered by MiCA. Meanwhile, the inherent risk exposure should continue to be regarded as high, due to the characteristics of crypto-assets and virtual currencies (internet-based, cross-border and anonymous). Therefore, the level of money laundering vulnerability related to crypto-assets and virtual currencies is considered very significant (level 4).

Risk level

As regards terrorist financing, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as very significant (4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant (4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both money laundering and terrorist financing is level 4, VERY HIGH.

Mitigating measures

For the competent authorities:

- Europol should consider
    - using blockchain analysis tools in order to analyse addresses and transactions for critical information such as geolocation data or the cryptocurrency exchange (used to purchase the coins);
    - the use of coinbase services offered to the law enforcement community. EU Member States could cross check their operational data (selectors) with coinbase (one of the largest exchangers) and receive useful information on entities/ persons/ IP addresses/ Bitcoins addresses.
- Competent authorities should continue their outreach to the crypto-assets services providers sector to raise awareness and understanding of new AML/CFT requirements, and promote expertise on these requirement also in the public sector.
- Competent authorities that have supervisory responsibilities over custodian wallet providers, and over providers engaged in exchange services between virtual and fiat currencies, should perform formal sectoral assessments of risks arising from such firms and promote risk awareness and guidance to the firms using available legal tools.
- Competent authorities should also consider the extent to which financial sectors they supervise are particularly exposed to the risks associated with crypto-assets, for example, because they accept firms dealing with crypto-assets as customers, and take steps to raise awareness of those risks as appropriate.
- Competent authorities should monitor developments in this area closely and assess whether changes to national legal and regulatory AML/CFT frameworks are required taking account of the EC legislative proposals highlighted above.
- Competent authorities should ensure that NFT sales platforms are covered under the categories of obliged entities submitted to their customer due diligence and other AML/CFT obligations.
- Competent authorities should further regulate DeFi applications to ensure they do not perform crypto-assets services providers while escaping the correspondent responsibilities as obliged entities, and reinforce the monitoring of their functioning to ensure there are no hidden management body that should be made liable for the activities of declared DEFIs.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

For the sector:

- Crypto-assets services providers should prepare themselves to an effective implementation of new AML/CFT obligations like the travel rule, including through the development of travel rule solutions.

For the Commission[133]:

- The Commission will assess suitable ways to complete its regulatory framework so as to ensure that crypto-assets and all crypto-assets service providers are properly covered by anti-money laundering obligations and notably the FATF travel rule on information accompanying crypto-assets transfers.

[133] The Commission is currently considering a proposal to subject crypto-currencies to automatic exchange of information for tax purposes:
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12632-Tax-fraud-evasion-strengthening-rules-on-administrative-cooperation-and-expanding-the-exchange-of-information_en

- The Commission will assess the possibility to give the Member States the possibility to require that crypto-assets services providers established on their territory in forms other than a branch and the head office of which is situated in another Member State to appoint a central contact point (as it is currently the case for Electronic money issuers and payment service providers).
- The Commission will assess the possibility to ban the opening, the custody and the use of anonymous crypto-assets wallets.
- In 2022, the Commission will issue a report on the implementation of AMLD5 and efforts by the Member States to implement the FATF standards.

12. Business loans

Product

Credit loans

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.

Additionally, loans between private entities constitute an important typology, often difficult to detect.

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, members of these organisations do not qualify for such loans (level of salary too low, funds originating from social benefits). This is confirmed by, in some cases, sanctioned entities (listed organisations) having tried to use business loans to finance terrorist activities through shell companies. Nevertheless this scheme requires a high level of expertise and knowledge. Further, competent national authorities found that TF risks can arise from consumer financing and the use of counterfeit identities or other frauds in loan application documents[134].

Conclusions: There is limited 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

While loan fraud (e.g. using strawmen, false documentation or establishing a fake loan to use a bank to transfer funds) are more common, incidents of laundering money through business loans have also been identified.

Europol's European Financial Intelligence Public Private Partnership (EFIPPP) information:

In relation to ML through real estate, various business loan schemes are known:

Loan-back schemes: Criminals lend each other money to purchase real estate using corporate vehicles they control, creating the appearance that the funds are legitimate and deriving from a real business activity. Examples: a) Inter-company loans of considerable amount without apparent business rationale used to purchase real estate, b) Use of payable-through accounts by which incoming payments from

[134] EBA's opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

abroad are immediately transferred without an apparent reason, c) Loans directly from offshore companies with no direct relation with borrower.

Back-to back Loans: A financial institution lends money or provides a guarantee based on the existence of collateral originating from illicit activities, such as illicit money deposited by the borrower. The bank is seen as the apparent lender, whereas the borrower is in fact borrowing from himself under the guise of a loan and is using these funds to finance the acquisition of real estate. Examples, a) Prospective buyer is paying for real estate with funds originating from offshore or secrecy jurisdictions, b) Real-estate loans above or equal to the building acquisition value.

Mortgage Schemes: a) Successive buying and selling of the real property involved, b) Borrower receives several mortgage loans relating to multiple properties.

In addition, the Covid-19 pandemic gave rise to new crime typologies, such as misuse of government funds, in particular in relation to the quick disbursement of Covid-relief funds which firms under pressure to pay out may be ill equipped to manage[135]. Some organised criminal groups have been active in providing loans to businesses in need by lending money during the COVID-19 crisis ("loan sharking"). Organised criminal groups target distressed companies with the view of later acquiring control over them and using them as a cover for their illegal ventures. Furthermore, criminals can acquire non-performing loans, using front-runners and front companies, and achieve the desired infiltration.

Further, perpetrators may be increasingly attempt to launder money through dormant companies, buy out financially the risk of loan fraud[136].

Conclusions: There is some 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 the money laundering vulnerability related to 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

[135] EBA's opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector, https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf.

[136] Europol's Serious and Organised Crime Assessment 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Financial institutions appear to be sufficiently aware of the risk of fraud that may arise in relation to business loans. The assessments are expected to be more thorough than for consumer loans, as the value of business loans are generally higher and financial institutions 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. However, more attention could be paid to remote onboarding solutions for Customer Due Diligence purposes. [137]

c) legal framework and checks

The regulatory requirements on business loans are robust as European rules (going beyond the AML/CFT framework) require financial institutions to take adequate measures, e.g. customer due diligence and ongoing monitoring, to identify the borrower and to address potential AML/CFT and credit risks. 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).

Risk level

As regards terrorist financing, both the levels of threat and vulnerability have been assessed as lowly significant (1).

	RISK	
➔	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

As regards money laundering, both the level of threat and the level of vulnerability have been assessed as moderately significant (2).

	RISK	
	1 – 1,5	Lowly significant LOW
➔	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing, is level 1, LOW and for money laundering it is level 2, MEDIUM.

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.
- NCAs should (on a comply-or-explain basis) monitor the mitigating measures suggested in the EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines')[138].
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

[137] See EBA's Risk Factors Guidelines: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

[138] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

13. Consumer credit and low-value loans

Product

Credit loans

Sector

Credit and financial sector

Description of the risk scenario

Members of terrorist/organised crime groups take out 'payday' loans (i.e. short term, low value but high interest loans), consumer credit or student loans. They also 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 credit.

These kind of loans can also be used to launder the proceeds of criminal activity. The loans can be 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 suggests that members of terrorist groups use this method to finance travel by foreign terrorist fighters to high risk non-EU countries. The most commonly used low-value product is consumer credit. The attraction of low value loans is that they do not necessarily require a high level of expertise or planning and the fact that credit providers need to process large number of loans every day.

As summarised by the EBA, the majority of competent authorities assessed the inherent ML/TF risk as moderately significant and only a limited number of NCAs found the risk to be significant or very significant. However, as the European AML/CFT regime does not require NCAs to cover also credit intermediaries, not all NCAs involved might have assessed this additional risk stemming from credit intermediaries with few direct contacts with their customers, and therefore potentially facing difficulties in ongoing monitoring and lack of oversight in the application of Customer Due Diligence (CDD) measures[139].

Conclusions: Consumer credit and low value loans are attractive for members of 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

Due to their low value, these products offer less money laundering potential than other financial products, but criminal organisations use them to finance the purchase of goods and then redeem the loans by cash. This might be even more problematic with quick consumer credit offered digitally, often

[139] See the Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

by non-bank lenders, since access becomes very fast and creditworthiness checks can be less thorough (e.g. because some products are exempted from legislative requirements or because supervision is more difficult)[140].

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 and have a limited cross-border dimension.[141] Nonetheless, 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 institutions and intermediaries that specialise in fast consumer loans, in particular due to the enhanced risk the usage of counterfeit identities that need appropriate assessments even when processing a high number of loan applications on a daily basis. CAs also noted that the sector was vulnerable to being used for terrorist financing purposes, as small amounts of credit can be obtained to finance terrorism[142].

b) risk awareness

This assumed low risk exposure is outweighed by the fact that, because of the small amounts and the high number of rapidly processed loans, risk awareness may be lower than for individual loan applications. In addition, as with business loans, there is more awareness of risks of fraud than of terrorist financing, so terrorist financing red flags may not necessarily be triggered. The IT systems in place are not necessarily equipped to detect forged documents.

Where credit or other financial institutions are involved, the terrorist financing checks can be considered robust as European rules (going beyond the AML/CFT framework) require these entities to take adequate measures, e.g. customer due diligence and ongoing monitoring, to identify the borrower and to address potential AML/CFT and credit risks. However, other credit intermediaries, that are currently not supervised, such as recent market entrants or telecommunications companies, are less aware of the risks and have less effective monitoring systems.

[140] See the Commission's Call for Advice to the ESAs on digital finance published in February 2021: https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/210202-call-advice-esas-digital-finance_en.pdf
The call focuses - among others – on non-bank lending and in particular on lending provided by financial intermediaries outside of the pan-European financial services regulatory perimeter, e.g. crowdfunding platforms facilitating the granting of credit to consumers – see p. 10-11.

[141] See Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

[142] See Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

c) legal framework and checks

While consumer credit/low-value loans provided by credit institutions or financial institutions are covered by the AML/CFT framework and other relevant sectoral legislation (e.g. CRD/CRR, CCD) at EU level, national legislations vary considerably as regards documentation requirements. Some Member States require specific documents, while others do not. In particular, the rules regulating the use of digital identities for digital customer identification and verification still vary due to a lack of harmonised requirements at EU level.

Conclusions: The volume of transactions and amounts at stake are usually low, but that does not reduce the inherent terrorist financing risk. The possible ineffective alert systems and checks in some firms that provide consumer credit may add to the terrorist financing vulnerability. Some new market entrants may also be less aware of terrorist financing risks as compared to incumbents (e.g. specialist lenders or the banking sector. The differences between national legislative frameworks show that the capacity of competent authorities and financial intelligence units to detect suspicious transactions may be 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 relatively low amounts associated with consumer credit, vulnerabilities can be high if, for instance, firms in the sector lack the proper monitoring systems to detect linked transactions or if customers can repay loans using cash payments. 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 are granted by non-financial institutions that are not subject to AML/CFT obligations – the so-called "non-banking lending".

Competent authorities have identified risks of fraud deriving from delivery channels that often involve agents, whom firms find harder 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 and the high number of rapidly processed loans, risk awareness may be lower than for individual loan applications. Again, risk awareness seems more oriented towards risks of fraud than of money laundering. Hence, money laundering red flags may not necessarily be triggered in the sector, especially in the event of early redemption of the loan. Where financial institutions are involved, money laundering checks may be considered more robust, but recent market entrants, such as telecommunications companies, are not subject to AML/CFT obligations, might be less aware of money laundering risks and may 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 and the required due diligence due to the current lack of a harmonised rulebook at EU level.

As regards other credit intermediaries that are currently not covered by the definition of obliged entities within the AML/CFT framework, some Member States require specific due diligence measures, while others do not. Both shortcomings of the current AML/CFT framework are being addressed by legislative proposals of the AML/CFT package published by the European Commission in July 2021.

Conclusion: While the patterns of transactions and amounts at stake limit the risk exposure of the sector, vulnerability may be higher where loans are granted by non-banking institutions. The differences between national legislative frameworks show that the capacity 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).

Risk level

As regards terrorist financing, both the levels of threat and vulnerability have been assessed as significant (3).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
➔	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

As regards money laundering, both the levels of threat and vulnerability have been assessed as moderately significant (2).

	RISK	
	1 – 1,5	Lowly significant LOW
➔	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing it is level 3, HIGH, and for money laundering is level 2, MEDIUM.

Mitigating measures

For Member States / competent authorities:

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

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.
- Remote on-boarding: In the AML package from July 2021, the European Commissions proposed amendments to the rules on Customer Due Diligence (CDD). The new rules should facilitate and strengthen secure remote customer onboarding, and have been designed to be coherent with the Commission's proposed amendment to the eIDAS Regulation in relation to a framework for a European Digital Identity, including European digital identity wallets and relevant trust service, in particular electronic attestations of attributes[143].
- Credit intermediaries that are not financial institutions are currently not subject to AML/CFT obligations at EU level, except in certain Member States. In order to close this regulatory loophole, the European Commission proposed that credit intermediaries and consumer credit providers,

[143] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.

regardless of whether they are licenced as credit or financial institutions, should be considered obliged entities under the revised AML/CFT framework[144].

- As highlighted by the EBA, prudential supervisors should pay attention to ML/TF risks within the context of the credit granting process of the institution. In particular, prudential supervisors are encouraged to assess that institutions have systems and controls in place to ensure funds used to repay loans are from legitimate sources. In this context, financial institutions should ensure that they comply with the national measures implementing the EBA guidelines on loan origination and monitoring, which – among others – require financial institutions to identify, assess and manage the ML/TF risk associated with the type of customers they serve, the lending products they provide, the geographies to which they are exposed and the distribution channels they use. They should consider the purpose of the credit and take risk-sensitive measures to understand if the funds used to repay the credit, including cash or equivalents provided as collateral, are from legitimate sources[145].
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

[144] Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft_en.pdf

[145] See EBA Guidelines on loan originating and monitoring from 29 May 2020: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/884283/EBA%20GL%202020%2006%20Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring.pdf

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

Product

Mortgage credits

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 of the credit agreement.

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.

According to the latest Europol report on serious and organised crime threat assessment in the European Union from April 2021, most criminal groups and networks (68%) use basic money laundering methods such as investing in property or high-value goods. While investments in real estate and high-value goods is a common way to disguise the origin of the criminally acquired funds (see separate fiche on real estate), the Europol report does not provide any indication as regards to an enhanced usage of mortgage or high-value asset backed credits. However, as regards fraud, it points out that the most common form of bank fraud is loan and mortgage fraud (e.g. using by recruiting straw persons and forged documents)[146].

Impact of the Covid-19 pandemic

The current economic climate may make real estate firms or their customers more susceptible to financial difficulties or other pressures, thus creating incentives to ignore or circumvent AML rules and other controls. Less stringent controls by real estate operators and professionals may result in a higher risk of being exposed to mortgage-related fraud.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to mortgage credit shows that terrorist groups find this method 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 extensive documentation requested by creditors to the future borrowers as part of the creditworthiness assessment, or the ownership of real estate goods to sell. 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. Finally, buying an asset at an inflated

[146] Europol's Serious and Organised Crime Assessment 2021: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

price can still be a way to transfer big amounts of money, but the property valuation usually done by creditors should help mitigate this risk.

Conclusions: Mortgage credit requires a high level of knowledge and expertise to understand the product and provide the relevant documentation requested by the creditors to the future borrowers as part of the credit worthiness assessment (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.

Europol Financial Intelligence Public Private Partnership (EFIPPP) information - A known mortgage scheme:

Illicit actors obtain mortgage loans to buy properties. Illegal funds obtained subsequently are used to pay the interest or repay the principal on the loan, either as a lump sum or in instalments. The mortgaged funds are alternatively transferred to accounts offshore and presented as the legitimate source of the funds while the borrower defaults on the loan.
Indicators: Borrower provides forged documentation overestimating the market value of the property to purchase or renovate with the mortgage. Successive buying and selling of the real property involved. Borrower receives several mortgage loans relating to multiple properties. Establishment of trust accounts managed or in the custody of a third party to purchase properties and pay off mortgages.

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). Further, mortgage creditors and intermediaries that are not financial institutions are currently not subject to AML/CFT obligations at EU level they are subject to greater risks.

b) risk awareness

Awareness in credit institutions can be considered as satisfactory, however some shortcomings have been identified in some key checks performed by credit institutions.[147] 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 and a lack of full harmonisation of the current AMLD framework.

Further, EBA has highlighted that where a product allows payments from third parties that are neither associated with the product nor identified upfront, where such payments would not be expected, for example for mortgages or loans, and lending (including mortgages) secured against the value of assets in other jurisdictions, particularly countries where it is difficult to ascertain whether the customer has legitimate title to the collateral, or where the identities of parties guaranteeing the loan are hard to verify may contribute to increasing risk.

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 (e.g. information checked as part of the credit worthiness assessment, verification of the source of collateral, and tax or financial statements on the borrower). In addition, other participants in the process (such as notaries) can contribute to further mitigating the risk. In addition, EBA has provided further guidance factors that may contribute to reducing the AML/CFT risk for mortgages. [148]

Conclusion: 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).

[147] See Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

[148] See EBA Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/84: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

Risk level

As regards terrorist financing, both the levels of threat and vulnerability have been assessed as lowly significant (1).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderately significant (2), whereas the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing it is level 1, LOW, and for money laundering is level 3, MEDIUM.

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.
- Mortgage creditors and intermediaries that are not financial institutions are currently not subject to AML/CFT obligations at EU level, but in certain Member States. In order to close this regulatory loophole the European Commission proposed that mortgage credit intermediaries and consumer credit providers regardless of whether they are licenced as credit or financial institutions should be considered obliged entities under the revised AML/CFT framework[149].
- As highlighted by the EBA, prudential supervisors should pay attention to ML/TF risks within the context of the credit granting process of the institution. In particular, prudential supervisors are encouraged to assess that institutions have systems and controls in place to ensure funds used to repay loans are from legitimate sources. In this context, financial institutions should pay intention to comply with the national measures implementing the EBA guidelines on loan origination and monitoring, which – among others – require financial institutions to identify, assess and manage the ML/TF risk associated with the type of customers they serve, the lending products they provide, the geographies to which they are exposed and the distribution channels they use. They should consider the purpose of the credit and take risk-sensitive measures to understand if the funds used to repay the credit, including cash or equivalents provided as collateral, are from legitimate sources[150].
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

[149] Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft_en.pdf

[150] EBA Guidelines on loan originating and monitoring from May 2020: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/884283/EBA%20GL%202020%2006%20Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring.pdf

15. 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 EIOPA statistical database[151], the total reported assets of insurance corporations in the euro area for end of 2019 were EUR 12.706 billion covering EUR 11.105 billion of liabilities. Around EUR 9.009 billion is allocated to life insurance obligations. EU life premiums amounted to EUR 938 billion in 2019.

In addition to the AMLD (and in the future AMLR), specific provisions in the sectoral legislation 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 can use life-insurance products to fund their activities. The ML/TF risk mainly stems from the investment related components, such as paying a high one-off premium or capital accumulation. In addition, life policies can be redeemed early to generate lump sums and the proceeds can be transferred to other beneficiaries.

Europol Financial Intelligence Public Private Partnership (EFIPPP) information in relation to investment fraud typology:

Promotions of variable annuities and indexed universal life policies with complex and hard-to-understand structures are mentioned as an indicator for so-called boiler room schemes. In those schemes, scammers take advantage of the recent decline in asset prices to sell fraudulent investments in gold, silver and other commodities labelled as a safe haven as well as low value stocks or high risk financial products such as derivative instruments and cryptocurrencies.

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 or retirement benefit products as such).

[151] https://www.eiopa.europa.eu/tools-and-data/insurance-statistics_en

The risks may arise where:

- an insurer* accepts a premium payment in cash (this is not a common practice);
- an insurer refunds premiums, upon policy cancellation or surrender, including when the premium is refunded to an account other than the source of the original funding (owned by a party other than the policyholder);
- the insurer fails to establish the source of investments on a risk sensitive basis;
- an insurer sells transferable policies (these are uncommon);
- investment transactions involve trusts, mandate holders, etc.;
- an insurer sells a small investment policy initially and the investor makes subsequent large investments without undergoing additional 'know your customer' due diligence;
- complex distribution channels are used (e.g. long chains of intermediaries, no face-to-face sales).

One of the specific TF risks associated with the life insurance products is that a beneficiary does not have to be identified and verified at the outset of the business relationship. So often the beneficiary of a life insurance policy is someone else than the customer. He/she only needs to be identified and verified at the payout stage.

There is a money laundering risk in all of the above scenarios. Perpetrators use risk scenarios 1 and 6 for placement, 2, 4 and 7 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. Further, life insurances are mostly designed for the long term or verifiable event, such as death or retirement and thus provide limited flexibility. 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 do not allow this type of clause. Therefore, this risk is limited.

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 perpetuators 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 placing of funds rather than their withdrawal. However, the risk exposure seems limited, given the volume of transactions concerned and the limited flexibility of these products. 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.[152]

b) risk awareness

The sector seems quite unaware of terrorist financing risks. Even though life insurers, as other obliged entities are required to continuously screen their customer database against PEP lists and high risk country lists 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. Further, insurance companies often do not have client relationships with beneficiaries of the insurance policies and thus have access to much less information about their customers and beneficiaries 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'. In the future, this risk could be addressed by further measures to identifying the beneficiary[153].

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 the effectiveness of transaction 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 placing of funds and the capital accumulation, rather than their withdrawal. However, the risk exposure seems rather limited, given the volume of

[152] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector: file:///U:/AML/13.%20Policy%20applic%20-%20vulnerabilities%20&%20risks/Supranational%20risk%20assessment/SNRA%203%202019%20-%202021/00%20-%20BACKGROUND%20(EU%20WORK)/EBA%20Opinion%20on%20MLTF%20risks.pdf

[153] See the package of legislative proposals to strengthen the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules: https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en.

transactions concerned. Most competent authorities assess the overall level of inherent money laundering risk as being of low or moderate significance. A small number of competent authorities, however, considered that the risk was significant and that the quality of the controls of insurance undertakings from an AML/CFT perspective could be improved. They consider the sector's exposure to the money laundering risks arising from cross-border transactions and activities to be less significant[154].

b) risk awareness

The sector is well aware of the money laundering risks. However, as insurance companies often do not have client relationships with beneficiaries of the insurance policies they typically have access to much less information about their customers' transactions than other sectors (e.g. banks), which reduces their ability to build up comprehensive customer risk profiles.[155]

c) legal framework and checks

Customers are generally required to forward their investments to the insurance undertaking via their common bank accounts, which fall under the general requirements of the AMLD framework. 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 the effectiveness of transaction 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.

Conclusion: 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.

[154] Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector:
file:///U:/AML/13.%20Policy%20applic%20-%20vulnerabilities%20&%20risks/Supranational%20risk%20assessment/SNRA%203%202019%20-%202021/00%20-%20BACKGROUND%20(EU%20WORK)/EBA%20Opinion%20on%20MLTF%20risks.pdf

[155] See the package of legislative proposals to strengthen the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules:
https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en

Risk level

As regards terrorist financing, the level of threat has been assessed as moderately significant (2), whereas the level of vulnerability has been assessed as low/moderately significant (1/2).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderately significant (2), whereas the level of vulnerability has been assessed as low/moderately significant (1/2).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, money laundering and terrorist financing, is level 2, MEDIUM.

Mitigating measures

- Insurance undertakings should be able to identify higher risk situations, such as when the proceeds of the policy benefit a politically exposed person. To determine whether this is the case, the Commission presented a proposal in July 2021 that would require insurance policies to include reasonable measures to identify the beneficiary, as if this person were a new client. Such measures should be taken at the time of the payout or at the time of the assignment of the policy, but not later. Where there are higher risks identified, obliged entities shall: (a) inform senior management before payout of policy proceeds; (b) conduct enhanced scrutiny of the entire business relationship with the policyholder[156].
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol. Other risk mitigating measures can be found in EBA's sectoral guideline for life insurance undertakings[157].

[156] Proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing: https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft_en.pdf

[157] See EBA's ML/TF Risk Factors Guidelines' under Articles 17 and 18(4) of Directive (EU) 2015/849, para. 14.1 et seq: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

16. 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 EIOPA statistical database[158], the total reported assets of insurance corporations in the euro area for end of 2019 were EUR 12.706 billion covering EUR 11.105 billion of liabilities. Around EUR 820 billion of those liabilities is allocated to non-life insurance obligations.

At EEA level the most dominant non-life line of business is fire and other damage to property (Gross written premiums of EUR 152 billion over 2019), followed by medical expense (GWP of EUR 152 billion) and motor vehicle liability (GWP of EUR 98 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'.*

[158] https://www.eiopa.europa.eu/tools-and-data/insurance-statistics_en

European Financial Intelligence Public Private Partnership (EFIPPP) information:

In relation to investment fraud, a possible victim indicator of so-called boiler room schemes is the transfer of funds to third parties related to fees for insurance, bank services, lawyers, notary and other.

Also, in relation to ransomware and cryptocurrencies, an indicator of ransomware payments is payments from an organization – in particular from a sector at high risk for targeting by ransomware - to Digital Forensics and Incident Response (DFIR) firm or Cyber Insurance Company (CIC) specializing in assisting victims of ransomware attacks.

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.

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 of low significance (level 1).

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 limited evidence of non-life insurance being used to launder the proceeds of crime[159].

Conclusions: Non-life insurance is generally 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 (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 main situations may occur:

i. fictitious claims in motor vehicle retail /
ii. car insurance fraud: funds from the fraud are sent by cash transfer.

a) risk exposure

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

[159] See FATF Risk-based Approach Guidance for the Life Insurance Sector, para. 6: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-life-insurance.html

b) risk awareness

In general, non-life insurance could be more vulnerable than life insurance, not because of its business model but because the sector is not necessarily aware of the risks (customer due diligence is not implemented and there is no record-keeping) and 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, and to insurance fraud more broadly.

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

As usually prior identification is necessary for the transfer of funds, the risk is limited. However, non-life insurance can be 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).

Risk level

As regards terrorist financing, the level of threat has been assessed as of low significance and the level of vulnerability as moderately significant (2).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the levels of threat and vulnerability have been assessed as lowly significant (1).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is level 2, MEDIUM, and for money laundering level 1, LOW.

Mitigating measures

No further proposal is made at this stage.

17. Safe custody services

Product

Safe custody services

Sector

Credit and financial sector and private security companies

Description of the risk scenario

Safe deposit boxes are viewed as a tool to store cash whilst implementing the three stages of money laundering (Placement, Layering and Integration). 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. Perpetrators can also buy the relevant services through front persons, thus rendering them directly or indirectly via a front person.

Threat

Terrorist financing

For the purpose of this Supranational Risk Assessment the terrorist financing threat related to safe custody services would be no different from the threat relating to organised crime and money laundering. Therefore, it is not being considered as different to the threat of abuse for the purpose of money laundering.

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 on the number of persons that have access to a safe deposit box are difficult to obtain, because safe custody services are also used for relatives, associates, friends, etc. 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. The ability to obtain a safe deposit box using fraudulent identification also adds another element of risk to the cash storage sector.

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. Risk rating is primarily due to the inability of safe custody services employees to obtain information relating to the contents of the boxes and customers having unlimited access to facilities.

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 money laundering arises at the time of the storage or only once the funds are inserted in the real economy[160]. 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 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[161]. 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.

[160] Indeed, if it is cash just deposited in those boxes, it cannot qualify as ML yet. What it is important is to know **where** those boxes are and **who** the beneficial owners are in order to be able to recovery those assets.
[161] However, it is very important to have an strict control on who accesses the boxes. Full identification and reporting in case of suspicion.

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).

Risk level

As regards terrorist financing, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant/ significant (level 2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant/ significant (level 2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, money laundering and terrorist financing is HIGH.

Mitigating measures

There already exist limited controls to overcome the privacy requirements in the safe deposit box sector. Nevertheless, consideration should be given to improving current identity verification processes and access monitoring capabilities to address that fact that **parties other than the initial customer** may deposit or collect funds.

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.
- Considering the cross-border nature of ML and TF, Member States should seek internal cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

NON-FINANCIAL PRODUCTS

1. (Legal arrangements including) Trusts

Product

Trusts

Sector

Non-financial products

Description of the sector

Recent money-laundering scandals confirm that legal entities and arrangements are a favourite vehicle employed by criminals to disguise the proceeds of crime as legitimate corporate trade, often through complex structures and networks, which hide the beneficial owners.

Trusts are legal arrangements originally developed in common law jurisdictions. Within a trust, a settlor transfers assets to a trustee, who exerts control over these assets in the interests of one or more beneficiaries as determined by the settlor. The assets held in the trust constitute a separate patrimony from that of the trustee, while other parties, such as the settlor and protector, may also exert some level of control or influence over it[162].

Other arrangements may emerge as similar to trust by structure or function. Like trusts, they enable a separation of legal and beneficial ownership of assets. This does not necessarily mean divisibility of ownership - a concept typical of common law but not recognised under civil law[163]. Rather, a mechanism where the property is entrusted to one person, who holds the title to it or manages it for the benefit of one or more other persons or for a specific purpose[164].

[162] European Commission, Report from the Commission to the European Parliament and the Council Assessing whether Member States Have Duly Identified and Made Subject to the Obligations of Directive (EU) 2015/849 All Trusts and Similar Legal Arrangements Governed under Their Laws, COM(2020) 560 final, p. 4. See also art. 2 of the Hague Trust Convention, establishing the following definition: "For the purposes of this Convention, the term "trust" refers to the legal relationships created - inter vivos or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose. A trust has the following characteristics: a) the assets constitute a separate fund and are not a part of the trustee's own estate; b) title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee; c) the trustee has the power and the duty, in respect of which he is accountable, to manage, employ or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law. The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust".

[163] Sandor, I. (2015) "The legal institution of the trust in the economy and law of Eastern European countries", European Scientific Journal April 2015 SPECIAL edition 1857 – 7881, p. 139-149.

[164] Sepp, K. (2017). "Legal Arrangements Similar to Trusts in Estonia under the EU's Anti-money-laundering Directive", Juridica International, 26 (56-65). See also Schmidt, K. (2016) "Trust as a Legislative Challenge: Bipolar Relation vs Quasi-Corporate Status? – Basic Trust Models in Legal Practice, Theory, and Legislation", *European Review of Private Law* 6, p. 995–1010; European Commission, Report from the Commission to the European Parliament and the Council Assessing whether Member States Have Duly Identified and Made Subject to the Obligations of Directive (EU) 2015/849 All Trusts and similar legal arrangements governed under Their Laws, COM(2020) 560 final, p. 3.

As commonly used within the Union, EU rules and FATF standards[165] point to the following arrangements as to be considered similar to trusts[166]:

- *Fiducies*;
- *Treuhand*;
- Svěřenský fond;

The Commission published an overview of legal arrangements notified by the Member States as having a similar structure or function to trusts[167], which resulted in a fragmented picture due to the complexity of identifying and classifying the legal arrangements at hand.

Sixteen Member States[168] indicated that no trusts or similar legal arrangements are governed by their laws, while the remaining Member States[169] notified trusts or similar legal arrangements being governed by their laws.

Threat

Terrorist financing

In general, there is little evidence to date that trusts and other type of legal arrangements have been misused for the purpose of financing terrorism. Possibly due to the costs associated with setting up these arrangements, they do not appear to be particularly attractive to groups that carry out TF activities. The configuration of fiduciary structures does not allow the rapid management or disposition of funds - that usually accompanies TF activities – and demands a series of requirements to be carried out – which makes it difficult to use these structures for TF purposes[170].

Conclusions: The terrorism financing threat relating to trusts and other legal arrangements is considered lowly/moderately significant (level 1/2).

[165] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership* and European Commission; FATF (October 2006), *The misuse of corporate vehicles, including trust and company service providers*; Report from the Commission to the European Parliament and the Council Assessing whether Member States Have Duly Identified and Made Subject to the Obligations of Directive (EU) 2015/849 All Trusts and similar legal arrangements governed under Their Laws, COM(2020) 560 final, p. 9.

[166] European Commission, Report from the Commission to the European Parliament and the Council Assessing whether Member States Have Duly Identified and Made Subject to the Obligations of Directive (EU) 2015/849 All Trusts and similar legal arrangements governed under Their Laws, COM(2020) 560 final, p. 6-9; OJ 2019/C 360/05.

[167] See European Commission, Report from the Commission to the European Parliament and the Council Assessing whether Member States Have Duly Identified and Made Subject to the Obligations of Directive (EU) 2015/849 All Trusts and similar legal arrangements governed under Their Laws, COM(2020) 560 final.

[168] Austria, Belgium, Bulgaria, Croatia, Denmark, Estonia, Finland, Greece, Latvia, Lithuania, Poland, Portugal, Spain, Slovakia, Slovenia and Sweden. While this is also the case for Portugal, a specific provision under Portuguese law recognises foreign trusts and allows them to perform business activities exclusively in the Madeira Free Trade Zone. (Decree-Law 352-A/88, amended by Decree-Law 264/90).

[169] More specifically: 1. Cyprus, Ireland, Malta and the United Kingdom notified that trusts are governed under their legal systems, and Italy, Luxembourg and the Netherlands notified that trusts are recognised in their territory based on the provisions of the Hague Convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition: https://www.hcch.net/en/instruments/conventions/status-table/?cid=59
2. Czech Republic, France, Hungary, Italy, Luxembourg, Romania and the Netherlands notified similar arrangements governed under their national law; 3. Germany and Italy notified legal arrangements that are not expressly regulated in their national law, but are based on the general principle of the autonomy of the contracting parties and delimited by jurisprudence and doctrine. For the purpose of transposing Article 31 of the AMLD, Germany explicitly mentioned the above arrangements in its anti-money laundering law.

[170] NRA ES 2020 and NRA IE 2020.

Money laundering

Perpetrators can make use of trusts and similar legal arrangements in order to increase opacity within money laundering operations, by hiding the link with the real beneficial owner.

A recent study estimates that, on average, "1.2% of limited companies in the EU Member States, UK and Switzerland are controlled by a trust, a fiduciary or another legal arrangement that does not allow the beneficial owners to be identified. In some countries, such as the Netherlands (25.6%) and Luxembourg (8.7%), the percentage is much higher"[171].

Cases, as reported below, show that trusts and similar legal arrangements can be misused in order to hide (personal) assets from being detected, frozen and confiscated, and to commit tax crimes[172] and cross-border operations of money laundering.

Additionally, the risks of misusing trusts seems to increase when several participants to the trust coincide with the same natural or legal person, or when trusts are set up under the law of a foreign jurisdictions (so-called, foreign trusts)[173]. Due to the potential lack of coordination and exchange of information between national authorities, foreign trusts can make the most of the differing treatment of these legal arrangements by different Member States[174] and put transparency particularly at risk[175]. A related risk is the use of intermediaries to hide the existence of a trust established in another jurisdiction in order to prevent its detection by a Member State - where a rigorous system of due diligence and communication by the obliged entities may apply[176].

The case-studies presented below highlight some of the main ML threats posed by the misuse of trusts. In particular:

- In-depth analysis of trust deeds reveal the truth on ultimate control by paying attention to attribution of certain powers to the settlor;
- Enhanced anonymity offered by trusts and similar legal arrangements can provide significant benefits to criminal operations;
- Almost all of the cases involving the use of legal arrangements also involve company or other legal entities. Trusts and similar legal arrangements are rarely used in isolation to hold assets and obscure beneficial owners, but they generally are part of a wider scheme;
- Client is reluctant or unable to explain their source of wealth/funds;
- Legal person or arrangement incorporated/formed in a low-tax jurisdiction or international trade or financial centre;
- Focused on aggressive tax minimisation strategies;
- Correct documents not filed with the tax authority;
- Falsified paper trail;

[171] *EU SNRA 2021, Contribution/Input on the methodological approach*, Transcrime – Università Cattolica del Sacro Cuore (March 2021).
[172] FIU FR p. 70; NRA IT ("al fine di sottrarsi fraudolentemente al pagamento delle imposte, disponeva una donazione di immobili a favore di un trust, servendosi delle prestazioni di un avvocato quale trustee").
[173] NRA LU 2020.
[174] NRA ES; NRA UK; FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 24.
[175] NRA IT.
[176] NRA ES 2020.

- Funds involved in the transaction are sent to, or received from, a low-tax jurisdiction or international trade or finance centre.

MISUSE OF FOREIGN TRUSTS[177]
Following a complex criminal police investigation, authorities carried out the preventive seizure of funds, which were held in the offshore area of the Channel Islands (UK), traceable to a single family for a total value of over 1.3 billion euros. These financial assets had been unlawfully concealed by establishing a complex network of trusts. More specifically, Y trust in Member State A held a bank account in Alfa bank (in the same country) and had availability of over 6 million euros based on a fiduciary mandate. Beneficial owners of Y trust were all belonging to the same family (Family G). The legal representative of Y trust was an individual national in another country (Mr. Why), who had the same role in another trust (X trust) based in third country but domiciled in Member State A. X trust and Y were domiciled at the same address in country A, at which also a trust company (K) was registered. In depth analysis of the documents acquired allowed investigators to understand that Y and X trusts were merely formal shell and Mr. Why was a mere formal nominee. They had legal ownership of the assets, but they were strictly conditioned by Family G members (who were the real beneficial owner). The fiduciary mandate gave the settlor the right to dispose and enjoy of the assets, making Mr G the ultimate beneficial owner. Beneficiaries and settlors were always Family G members. Further, behind X and Y trusts there was a huge net of other trusts all linked to the Family G, establishing a complex net of control involving also companies established in other Member States. Such a complexity was not required by the purpose of the economic affairs. Thus, it had no commercial sense. In 2009 the fiduciary mandate of Y trust was transferred from the trust company K to Alfa bank, but it was not registered for tax purposes (despite this being mandatory). The aim was to legally repatriate the funds through a tax amnesty in 2009, while the use of a different trust company (Alfa rather than K) had the aim to obscure the relation between the assets and beneficial owners. All in all, the main points of the case are the following: - Expatriation of capital abroad segregated in a net of trust and multilevel of ownership by the same G family. Between 1995 and 2006, through complex corporate operations involving shares held by companies established in different Member States, the mentioned subjects were able to transfer assets to different trusts opened in the Channel Islands; - Ultimate owner control was on Mr. G family; - The funds were finally legally repatriated in 2009 via tax amnesty; - In order to conceal the beneficial owners, the in-bound funds were diverted to another trust company by the transfer of the fiduciary mandate, which was not notified to the tax register;

[177] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 35.

Investigation ended in seizure of the total assets held by the net of trusts. Those assets were the proceeds of multiple crimes, such as aggravated embezzlement to the detriment of certain companies, tax fraud, breach of trust, and false corporate communications.

In addition, technical investigations allowed to gather evidence against chartered accountants who, through their financial and tax consultancy, had over time facilitated the establishment of the above capitals and the screening thereof through the trusts, with the aim of facilitating laundering and reinvestment.

MISUSE OF FUNDS THROUGH A FOUNDATION[178]

Natural persons repatriated to a Member State funds originating from accounts in a foreign jurisdiction in the name of two Stiftung and an AG corporation with address in that jurisdiction and a Ltd. corporation with its address in another jurisdiction, as well as in the name of trustees of a trust in that jurisdiction. The repatriated funds were used for various payments and purchases. Inadequate justification of the source of funds led to a suspicion of serious fiscal fraud.

OBFUSCATION OF THE ORIGIN OF FUNDS THROUGH FOREIGN TRUST[179]

Mr Y was the manager of a French antiques gallery (Gallery A). In 3 years, Gallery A's bank account was credited with EUR 7 million from a trust registered in a foreign country. Most of the funds, EUR 5 million, were transferred to several European galleries to finance the purchase of artworks. Of this amount, only three transactions, totalling EUR 2 million, were the subject of declarations of trade in goods filed with the customs services. The remaining EUR 3 million was transferred to another gallery, Gallery B, whose manager was suspected by his country's legal authorities of being involved in dealing in stolen antiques.

The invoices for the purchase of antiques by Gallery A from Gallery B contained irregularities: the VAT number was not valid for cross-border transactions in the EU and was linked to a company that has been inactive since 2014. The transactions between the two galleries were not declared to the customs authorities. Lastly, EUR 150,000 credited to Mr Y's account from Gallery A's account was withdrawn in cash. These funds could have been used to finance an undeclared commercial activity. The elements described above could constitute tax fraud and tax laundering and are likely to be part of efforts to launder the proceeds of art trafficking.

Conclusions: The money laundering threat relating to trusts and other legal arrangements is considered very significant (level 4)

[178] *Ibid*., page 117.
[179] Tracfin, *ML/TF risk trends and analysis in 2019-2020*, page 44-45.

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerabilities posed by legal arrangements has been considered together with money laundering schemes related to legal arrangements. There are indeed no indications that vulnerabilities vary in type or intensity according to the type of misuse.

Conclusions: The terrorist financing vulnerability relating to trusts and other legal arrangements is considered significant (level 3).

Money Laundering

A recent report by the FATF notes that "the complex structure of trusts makes the identification of the beneficial owners difficult, and requires further efforts to determine the true nature of the trust relationship"[180].

Generally, a trust can be used for a variety of goals. For example, transferring the administration of an asset to a third party to organise an inheritance; protecting assets for children; or investing and accumulate money for future important expenses (such as education fees or retirement)[181].

However, trusts and similar legal arrangements can be also misused to enhance anonymity by adding an additional layer of complexity through the separation of the legal and beneficial ownership of an asset. The enhanced anonymity offered by trusts and similar arrangements can provide significant benefits and can present challenges to financial transparency. The ability to disconnect legal from beneficial ownership presents a range of challenges for authorities and service providers seeking to determine beneficial ownership. Additionally, trusts may be used by criminals as part of complex and opaque structures, comprising multiple legal entities and arrangements across multiple jurisdictions, which can be used to obscure who owns and controls assets[182].

This concern is even greater with respect to the risks linked to certain types of trusts or similar structures, such as those that[183]:

- Have one or more natural or legal persons or legal instruments in the chain of control, in most cases in order to make it difficult to detect the beneficial owner of that structure and the origin of the funds and assets managed;
- Have a purely instrumental character, meaning that they are owners (mere holders) of assets, but do not perform asset management activities of a commercial or financial nature;
- Have been incorporated in certain higher risk jurisdictions without apparent economic justification (vehicles off-shore corporations, shell companies, intervention of nominal holders etc.);

[180] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*.
[181] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 23.
[182] FIU IT; NRA EI p. 44; FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 61("[…] particularly TCSPs offer directorship, virtual office and mailbox services. These services allow the legal person to maintain a physical footprint in a country, and can distance the legal person from other assets and activities controlled by the beneficial owner. As a result, these services are vulnerable to exploitation for the purpose of disguising the true controllers and beneficial owners of a legal person, its assets, and its transactions. […] TCSPs represented the large majority of intermediaries involved in the provision of these services").
[183] NRA ES 2020.

- Carry out operations, including payments and collections, without a clear connection with the purpose of the trust;
- Are configured as an asset protection trust.

Conclusions: The money laundering vulnerability relating to trusts and other legal arrangements is considered significant (level 4).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as lowly/moderately significant (1/2), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

Conclusions: the estimated risk level for terrorist financing is MEDIUM and for money laundering VERY HIGH.

Many threats and vulnerabilities for money laundering have been identified in relation to (domestic and foreign) trusts and similar legal arrangements. They are to be considered as lucrative tools to lauder the proceeds of crime. Considering also the weaknesses in the mitigating measures, the level of money laundering risk is assessed as very high.

In contrast, there is little evidence that trusts and similar legal arrangements have been misused for the purpose of financing terrorism. However, their secrecy and the possibility to use them in combination to legal entities make trusts and similar legal arrangements vulnerable to abuse for terrorist-financing purposes. Thus, the level of risk here is assessed as medium.

Mitigating measures

In light of the above-mentioned risks and vulnerabilities, it is essential to stress that the integrity of the EU financial system depends on the transparency of trusts and similar legal arrangements.

For this reason, the EU has always been committed to implement an effective AML/CTF framework, specifically targeting the main issues related to trusts and alike arrangements.

In this context, and going beyond 2012 FATF Recommendations, since 2015 the EU adopted:

- Directive (EU) 2018/843[184], the 5th AMLD (Amendments to the 4th AMLD);
- Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds[185] in order to make fund transfers more transparent and to help law enforcement authorities to track down terrorists and criminals;
- Directive 2018/822/EU[186] which requires intermediaries to submit information on reportable cross-border tax arrangements to their national authorities comes into effect as from 2020.

In particular, Article 31 AMLD requires trustees or persons holding an equivalent position in a similar legal arrangement to:

- Obtain and hold adequate, accurate and up-to-date information on the arrangement's beneficial ownership;
- Disclose their status and provide information on the arrangement's beneficial ownership to obliged entities in a timely manner;
- Submit information on the arrangement's beneficial ownership to the central beneficial ownership register set up in the country where the trustee is established or resides, or the country where the arrangement enters into a business relationship or acquires real estate when the trustee is established or resides outside the EU; and
- Provide proof of registration in the central beneficial ownership register or an excerpt of it when wishing to enter into a business relationship in another Member State.

The AMLD also obliges Member States to establish effective, proportionate and dissuasive measures or sanctions for breaches of the above obligations.

Based on the information reported by the Member States, the above mentioned obligations have been implemented or are in the process of being implemented. However, implementation has been particularly problematic in relation to art. 31 AMLD para. 1, 2, 3, 4, 5, 7, 9.

Further, violations of CDD and reporting obligations by trust companies and services providers (TCSPs) have been reported in Member States. Such breaches of EU and national AML regulations included lack of identification of the clients; lack of identification of beneficial owners; and lack of reporting suspicious transactions[187].

Therefore, the following mitigating measures remain a priority for Member States and competent authorities:

- Carry out a review of arrangements that can develop by virtue of law or legal tradition to ensure that all persons managing trust-like arrangements are requested to report the natural persons that are parties

[184] 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.*

[185] 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.*

[186] 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.*

[187] NRA IT ("Ispezione nei confronti di un trust company, a seguito della quale sono state riscontrate numerose e ripetute violazioni agli obblighi antiriciclaggio, con particolare riferimento a quelli di identificazione dei clienti e dei titolari effettivi, nonché di registrazione delle operazioni via via eseguite. Nel corso delle attività ispettive è stata altresì rilevata la mancata segnalazione di un'operazione sospetta di circa 43,2 milioni di euro").

to the legal arrangement (or beneficiaries to those parties) to the register of beneficial ownership of trusts and similar legal arrangements.

- Develop a methodology for the risk assessment of legal arrangements.
- Ensure that beneficial ownership registers are fully populated and that there are mechanisms in place so that the information they contain is adequate, accurate and up-to-date.
- Provide outreach / training sessions to obliged entities on identification of beneficial owners and risks associated with business relationships and occasional transactions with legal arrangements, with a focus on non-face-to-face business relationships, offshore professional intermediaries and non-EU customers.
- Supervisors should conduct thematic inspections on how beneficial ownership identification requirements are implemented.
- As regards offshore trusts, consideration should be given to introducing
    - the obligation for holders of foreign trusts to declare them in their Member States (if this obligation does not yet exists);
    - more strict reporting requirements for transactions with foreign trusts, and
    - enhanced international cooperation.

2. Nominees[188]

Product

Nominees

Sector

Non-financial products

Description of the sector

Having in mind the distinction between informal nominees (*e.g.*, strawmen) and formal nominees (*i.e.*, nominee directors and nominee shareholders[189]), this fiche covers the latter category only.

A nominee director exercises the functions of the director in the company on behalf of (and subject to the instructions of) the nominator. The nominee typically signs a general power of attorney giving the nominator full power to manage the entity and generally also provides a signed and undated letter of resignation to further protect the nominator's anonymity[190].

A nominee shareholder exercises the associated voting rights according to the instructions of the nominator and receives dividends on behalf of the nominator. Because the identity of the nominator is not evident, the identity of the person behind the nominee shareholder can be concealed.

According to an investigation conducted by The Guardian, more than 21,500 companies worldwide used 28 nominee directors located in a few jurisdictions who played a key role in concealing hundreds of thousands of commercial transactions. They sold their names with addresses located all over the world for use on official company documents to appear as directors of those companies[191]. Also, literature reports that "due to the need for secrecy and deceit in money laundering, it is likely that many of these companies are engaged in some sort of criminal activity"[192].

Legally, nominees are responsible for the operation of the company, and accept the legal obligations associated with company directorship or ownership in the country in which the company is incorporated[193].

The providers of trust and company services (TCSP sector) are likely to provide nominee and directorship services, among others, to third companies[194].

---

[188] This analysis focuses on appointing nominee directors and nominee shareholders as one of the higher risk activities of Trust and Company Service Providers (TCSPs).

[189] "Formal nominee arrangement means a contract or a formal arrangement with an equivalent legal value to a contract, between the nominee and the nominator, where the nominator is a legal entity or natural person that issues instructions to a nominee to act on their behalf in a certain capacity and the nominee is a legal entity or natural person instructed by the nominator to act on their behalf. Nominee arrangements include nominee directors and nominee shareholders" (EU AMLR 2021).

[190] Pacini C., Stowell N., *Panama Papers and the Abuse of Shell Entities:* https://www.emerald.com/insight/content/doi/10.1108/978-1-78973-417-120201023/full/pdf?title=panama-papers-and-the-abuse-of-shell-entities

[191] James Ball, *Offshore Secrets: How Many Companies Do 'Sham Directors' Control?*, The Guardian (2012): https://www.theguardian.com/uk/datablog/2012/nov/26/offshore-secrets-companies-sham-directors https://perma.cc/376U-N5KT

[192] Pacini et al., *An Analysis of Money Laundering, Shell Entities, and No Ownership Transparency that Washes Off and on Many Shores: a Building Tidal Wave of Policy Responses*, KAN. J.L. & PUB. POL'Y, Vol. XXX:1 (2020).

[193] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 7.

[194] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 7.

The law on nominees changes from one Member State to another and no exhaustive overview exists at EU level. A partial view can be derived from information submitted to the Commission by Member States, which indicates that nominee directors are not allowed in 12 Member States[195] and explicitly allowed in one Member State[196] only, while some other Member States[197] do not recognise or define the role explicitly. With reference to nominee shareholders, 8 Member States[198] allow them, while 7[199] do not. Some others do not recognize or explicitly define the concept[200].

Threat

Terrorist financing

In general, there is little evidence to date that formal nominees have been misused for the purpose of financing terrorism. They do not appear to be particularly attractive to groups that carry out TF activities.

Conclusions: The terrorist financing threat relating to nominee services is considered lowly/moderately significant (level 2).

Money laundering

Nominees have been used to disguise ownership and control, or to circumvent laws designed to manage foreign business ownership and foreign trade.

According to a FATF study, FIUs and law enforcement agencies report the use of nominee services by known criminals and individuals who have been prohibited from serving as a director of a company due to previous malfeasance. Criminals have been known to recruit people with no criminal history to perform these roles, or who agree for their details to be recorded in these positions. The presence of nominee directors and shareholders in company records can also affect law enforcement investigations by delaying the identification of the beneficial owner, or by creating false links between companies that share nominees[201].

Nominees are also often provided as a service in offshore situations. In this case, third-party nominee services are often used as a means to protect the confidentiality of a nominator whose name can be kept off company registration documents and public registries[202]. In many cases, the nominator will maintain some level of direct control in a scheme, but usually by means of an intermediary or a nominee[203]. This could include shareholders and directors, such as spouses, children, extended family, and other personal or business associates.

The Panama Papers and other recent scandals have shown how nominees can be misused to disconnect the assets from their real owner and disguise the identity of the beneficial owner[204].

[195] Austria, Czech Republic, Germany, Estonia, Spain, Finland, Hungary, Croatia, Italy, Sweden, Slovakia, the Netherlands.
[196] Cyprus.
[197] Slovenia, Poland, Malta, Latvia, Greece, Denmark, Bulgaria.
[198] Austria, Cyprus, Germany, Denmark, Finland, Hungary, Italy, Poland.
[199] Czech Republic, Estonia, Spain, Croatia, the Netherlands, Sweden, Slovakia.
[200] Bulgaria, Slovenia, Malta, Latvia, Greece.
[201] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 61.
[202] Pacini et al., *An Analysis of Money Laundering, Shell Entities, and No Ownership Transparency that Washes Off and on Many Shores: a Building Tidal Wave of Policy Responses*, KAN. J.L. & PUB. POL'Y, Vol. XXX:1 (2020).
[203] Del Mundo C., *How Countries Seek to Strengthen Anti-Money Laundering Laws in Response to the Panama Papers, and the Ethical Implications of Incentivizing Whistleblowers*, 40 NW. J. INT'l L. & Bus. 87 (2019).
[204] TI feedback.

Nominees can be involved in the structure of shell companies. Although no formal definition exists of shell companies, they are generally understood as not carrying out any substantial economic activities. They can be supported by means of TCSPs and nominee directors whose role in the management and direction of the company is limited[205].

Nominees can be involved also in private interest foundations (PIFs), which are "vehicles offered by code law nations and some common law countries for tax management, estate planning purposes, asset protection, and as an alternative to trusts"[206]. Finally, the use of nominees by companies in the gambling and betting sectors[207], as well as in employee share schemes[208], has been reported.

In contrast, a decrease in the provision of nominee services by investment funds has been registered by the European Banking Authority[209].

Case Study - Luxembourg[210]
International Company A headquartered in an EU jurisdiction made corrupt payments to a government employee using nominee director services and international transactions in the following way: • International Company B was registered in a foreign jurisdiction, with a government employee as the beneficial owner. • International Company B used nominee shareholders and directors provided by TCSPs, thereby permitting the concealment of the government employee's identity. • Payments were made via a European bank account of a subsidiary of International Company A to another of its accounts in Eastern Europe, and via an enterprise registered in Asia. These funds were then paid into bank accounts in a foreign jurisdiction. • The funds were transferred from the bank accounts in foreign jurisdiction to a Luxembourg bank account of International Company B, to which the government employee had access (being the BO).

Nominees acting on behalf of PEPs[211]
A politically exposed person (PEP) wants to invest in a property in France. Its objective is to invest while protecting its identity throughout the purchase process. The PEP proceeds to the purchase of a property in France via a Société Civile Immobilière (SCI)[212] domiciled in country B. The procedures for acquiring the property are then carried out by a nominee who is a national of country A, specializing in real estate investments. The nominee represents the SCI at the signing of the deed. The funds relating to the purchase reach the notary via a bank account located in country A. The anonymity of the beneficial owner is preserved by this scheme.

[205] FATF (2018), *Financial Action Task Force*; Pacini C., Stowell N., *Panama Papers and the Abuse of Shell Entities:* https://www.emerald.com/insight/content/doi/10.1108/978-1-78973-417-120201023/full/pdf?title=panama-papers-and-the-abuse-of-shell-entities; Banca d' Italia (December 2020), *Quaderni dell'antiriciclaggio: Un indicatore sintetico per individuare le società cosiddette cartiere*.

[206] Pacini C., Stowell N., *Panama Papers and the Abuse of Shell Entities:* https://www.emerald.com/insight/content/doi/10.1108/978-1-78973-417-120201023/full/pdf?title=panama-papers-and-the-abuse-of-shell-entities

[207] Banca d'Italia (January 2018), *Quaderni dell'antiriciclaggio dell'Unità di Informazione Finanziaria: Le linee di intervento della nuova regolamentazione antiriciclaggio nel settore del gioco*.

[208] LPLA NRA IE

[209] EBA (March 2021), *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector*.

[210] NRA LU 2020.

[211] https://blogavocat.fr/space/marie-lise.assouslegrand/content/lettre-dinformation-tracfin-octobre-2015

[212] An SCI is a rather specialist type of French company (*société*) that is constituted for the ownership and management of real estate (*immobilière*).

Nominees and organized crime[213]
Thanks to an investigation carried out in Italy, it was discovered that nominees were linked to companies established for money-laundering purposes by organized crime. 12 million euros value assets was confiscated by the Italian judicial authority.

A range of service providers are known to offer formal nominee services, including legal and accounting professionals, TCSPs, and professional nominees (people who rent their identification information to companies for nominee purposes only, but provide no additional services to the company)[214]. The case study below demonstrates how a TCSP provided nominee directorship services for over 1000 companies on behalf of foreign clients. Authorities suspected that such schemes facilitated crimes in foreign jurisdictions, including the smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering[215].

Conclusions: The money laundering threat relating to nominee services is considered very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerabilities posed by formal nominees has been considered together with money laundering schemes related to formal nominees given that ways in which nominees could be misused for terrorist financing purposes would be the same as those in which they could be misused for money laundering.

Conclusions: The terrorist financing vulnerability relating to nominee services is considered significant (level 2).

Money laundering

Based on the above, it becomes clear that the availability and use of formal nominee services are vulnerable to exploitation for the purposes of disguising beneficial ownership. As noted by the FATF, "nominees have been identified as a central enabler of indirect ownership chains"[216].

Nominee services can be used to facilitate money laundering[217], tax evasion, and corruption. The globalisation of trade and communications has only increased this threat, and countries now face the challenge of enforcing national laws in a borderless commercial environment[218]. Indeed, as the FATF notes, "nominee directors and shareholders are a key vulnerability. The role of the nominee, in many cases, is to protect or conceal the identity of the beneficial owner and controller of a company or asset. A nominee can help overcome jurisdictional controls on company ownership and circumvent directorship bans imposed by courts and government authorities. While the appointment of nominees is lawful in most countries, the

[213] https://www.gazzettinonline.it/2021/04/16/operazione-follow-the-money-ii-sequestro-preventivo-per-7-societa-per-un-valore-di-12-mln-di-euro-video_169127.html
[214] NRA IE.
[215] Ireland reports that despite nominee services being "generally considered to be a higher ML/TF risk, the risk is mitigated by the fact that TCSPs authorized by the Central Bank of Ireland are subsidiaries of regulated entities" (NRA IE).
[216] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 86.
[217] Including drug trafficking as a predicate offence for money laundering (BG SNRA).
[218] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 5.

ongoing merits of this practice are questionable in the context of the significant money laundering and terrorist financing vulnerabilities associated with their use"[219].

Conclusions: The money laundering vulnerability relating to nominee services is considered very significant (level 4).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as lowly/moderately significant (2), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the levels of threat and vulnerability have been assessed as very high (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

Many threats and vulnerabilities for money laundering have been identified in relation to the use of formal nominees. They are to be considered as lucrative tools to launder the proceeds of crime. Further, there is the risk that the current EU definition of beneficial owners leaves a loophole allowing for nominees acting as company directors to be reported as beneficial owners[220]. Therefore, the level of money laundering risk is assessed as very high.

In contrast, there is little evidence that formal nominees have been misused for the purpose of financing terrorism. However, the possibility to use them in combination to legal entities make nominees vulnerable to abuse for terrorist-financing purposes. Thus, the level of risk here is assessed as medium.

Conclusions: estimated risk level for terrorist financing is MEDIUM and for money laundering VERY HIGH.

Mitigating measures

Under the AML Directive, nominees have not been regulated. Even if not explicitly mentioned, nominee directors and nominee shareholders are included in the services provided by a trust company service provider as per article 3(7) of AMLD5. Furthermore, under Annex III of the AMLD "companies that have nominee shareholders" are to be considered as one of the customers risk factors of potentially higher risk that obliged entities should take into account when performing CDD.

[219] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 6.

[220] TI FEEDBACK (see folder on third parties feedback). TI recommended to: i) require nominees to be licensed, to disclose the identity of their nominator to the company and any other relevant registry and keep records of the person who appointed them; ii) explicitly forbid the possibility for nominees to be reported as beneficial owners; iii) apply effective sanctions whenever a nominee has been wrongly reported as a beneficial owner". However, the 2021 AML/CTF legislative package will include many of these proposals.

As mentioned in the description of the sector, in many Member States the use of nominee shareholders is not possible in light of the specific provisions of national company law. At the same time, proxy services that resemble nominee arrangement remain possible. Given the measures already implemented at EU level in terms of company and beneficial ownership transparency, the usage of formal nominee arrangements is more limited than other company services[221]. At the same time, overseas companies created under laws that allow nominee arrangements still present unaddressed risks. When it becomes possible to run such companies through offices in the EU, these risks enter the internal market.

In order to mitigate risks from nominee arrangements, Member States and competent authorities should:

- Provide that the status of nominee director, or proxy director, is disclosed as public information[222].
- Provide guidance/outreach to obliged entities to ensure they are able to detect nominee relationships in the ownership/control structure of their corporate clients.
- Monitor the business population to assess the prevalence of nominee relationships in companies' structures.

[221] See for example the analysis produced by Luxembourg's CSSF on nominee services in the sectoral ML/TF risk assessment for TCSPs, https://www.cssf.lu/wp-content/uploads/ML_TF_risk_analysis_TCSP.pdf, page 35

[222] As in publication on beneficial ownership registers for legal persons as well as any other relevant national database. According to FATF 2012 updated recommendations, the following are considered as mitigating measures:
(a) requiring nominee shareholders and directors to disclose their nominee status and the identity of their nominator to the company and to any relevant registry, and for this information to be included in the relevant register, and for the information to be obtained, held or recorded by the public authority or body or the alternative mechanism referred to in paragraph 7. Nominee status should be included in public information;
(b) requiring nominee shareholders and directors to be licensed, for their nominee status and the identity of their nominator to be obtained, held or recorded by the public authority or body or alternative mechanism referred to in paragraph 7 and for them to maintain information identifying their nominator and the natural person on whose behalf the nominee is ultimately acting, and make this information available to the competent authorities upon request; or
(c) enforcing a prohibition of the use of nominee shareholders or nominee directors.

3. Companies[223]

Product

Companies

Sector

Non-financial products

Description of the sector

According to the latest available statistical data[224], about 22,5 million companies exist in the EU. Companies can be classified in different categories according to their size. The European Union economy mainly relies on SMEs, which represent 99% of all business in the EU[225]. 94% of these companies is independent, meaning that they are neither controlled by another company nor do they control themselves another company[226]. According to a study conducted by Eurostat in 2015, dependent companies (those that are controlled by another company and/or control themselves another company, and thus belong to a group of companies) are important in terms of employment and turnover, especially in Denmark, Estonia, Latvia, Finland, Sweden and Norway. Therefore, a large proportion of total growth created by SMEs can be attributed to dependent companies[227]. Finally, in 2015 1.6 % of companies that were dependent companies belonged to an international group. Those companies contribute highly in terms of employment and turnover especially in Estonia, Latvia, Netherlands, Portugal, and Romania[228].

It is relevant to distinguish between partnerships and corporations[229]. In a partnership, all partners specified in the partnership contract exercise ownership and control. In contrast, the capital participation of shareholders is the focus of capital companies[230].

In a partnership, the absence of legal segregation between the natural persons and an independent legal person allows the direct exercise of management by the partners. This reduces the ability to misuse a partnership to disguise beneficial ownership[231].

---

[223] Apart from companies, legal persons also include other entities like foundations and, under EU AML framework, special consideration is given to foundations too. At international level, FATF has identified inadequate BO identification rules for foundations and Article 3(6)(c) of the AMLD establishes:

> *(…) in the case of legal entities such as foundations, and legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b);*

In this regard, the 2021 AML package proposes further enhancements in relation to quasi foundations and beneficial ownership requirements.

Also, the term 'companies' encompasses a wide range of businesses including lower risk entities like listed companies which are heavily regulated, this analysis doesn't cover those.

[224] Eurostat, Structural business statistics overview, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Structural_business_statistics_overview#Size_class_analysis

[225] European Commission, SME Definition, https://ec.europa.eu/growth/smes/sme-definition_en

[226] Eurostat, Statistic on Small and Medium-size enterprises, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises#Country_by_country_analysis

[227] Eurostat, Statistic on Small and Medium-size enterprises, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises#Country_by_country_analysis

[228] Eurostat, Statistic on Small and Medium-size enterprises, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises#Country_by_country_analysis

[229] ML/TF issues relate to unlisted companies like private limited liability companies, rather than listed companies.

[230] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 21.

[231] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 21; NL NRA on ML (2019); ES NRA.

Unlike partnerships, corporations are separate legal entities and are often controlled and owned through shares, which can be transferred and sold regularly without affecting the existence of the capital company itself. A company's legal personality allows it to conduct business and own assets under its own name, assuming all rights and being liable for all debts and obligations it enters into. This legal structure allows a natural person to take part in business without disclosure of their personal identity. Even though shareholders own the company, usually they are not actively involved in management functions, but instead elect or appoint a board of directors to manage the company in a fiduciary capacity. Such types of contract are usually not publicly available, thus allowing room to exploit nominees and obscure true ownership and control arrangements in order to obscure beneficial ownership [232].

Complex ownership and control structures in themselves are not unlawful. Often, these corporate structures serve legitimate purposes and facilitate a wide range of commercial activities, entrepreneurial ventures, and the management of personal finances. Complex ownership structures can simplify business transactions for companies that regularly trade transnationally, provide services to international clients, or conduct parts of a company's operations (such as manufacturing or research and development) in another country. However, complex structures can also be used to obscure beneficial ownership, avoid taxation obligations, conceal wealth, and launder the proceeds of crime. The majority of cases that involved tax evasion, fraudulent investment schemes and fraud also utilized complex structures to conceal beneficial ownership[233].

It is important to consider shell companies and front companies. Shell companies can be detected through a number of characteristics and indicators, including the use of only a post-box address, a lack of personnel, and a lack of payments in taxes and/or social benefit payments. Furthermore, many shell companies do not have a physical presence, and are geographically anchored through the use of TCSPs and nominee directors whose role in the management and direction of the shell company is limited[234]. A front company is a fully functioning company, with assets, income, expenses. Any functioning company can be a front company, but the most common form of front company is one that operates in the customer service industry (such as a restaurant, night club, or salon) as these businesses commonly handle cash[235].

Finally, offshore companies should be considered. This term describes a company with share capital, governed by private law, incorporated under foreign law and with legal personality that does not develop any economic activities within the jurisdiction in which the place of incorporation and/or registered office of the company is located, and of which the actual titleholder or holders resides or reside in a country other than where the company is established[236]. Moreover[237]:

- the government in the country of incorporation may not levy direct tax (although the offshore company is obliged to pay a fixed annual amount to the government);
- the offshore company may not have its own physical office address, personnel, means of communication and such;

[232] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 21. See also Van der Does de Willebois, E. et al. (2011: p. 162) who claims that companies are the most misused corporate vehicle documented in his study, especially to disguise ownership and control; ES NRA.
[233] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 27. See also ES NRA.
[234] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 29.
[235] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 30
[236] NL NRA on ML (2019).
[237] NL NRA on ML (2019).

- the offshore company may have an agent in the country of establishment (registered agent) and office address (registered office);
- the offshore company may be managed and administered by an employee of a local trust or law firm;
- often transactions take place only between affiliated companies within the same organizational structure.

Threat

Terrorist financing

There have been instances where companies have been abused for terrorist financing purposes (for example, in Ireland). Funds generated by criminal activities have been laundered through cash enterprises, such as licensed premises and security companies or in the form of "loans" to businesses. These were often fronted by persons with no obvious affiliations to terrorist groups and whose involvement in terrorist financing was found after investigation[238].

Case involving terrorist financing via foundations established in the Netherlands[239]
In November 2019, six men were arrested as part of an international investigation on terrorist financing in the Netherlands and Belgium. They had allegedly handed over funds to ISIS fighters or affiliated persons in Turkey and Syria in 2013-2014, where these funds had previously been collected via a foundation with the aim of helping war victims. There is reason to believe that the Dutch foundation raised at least EUR 200,000 in donations by organizing various gatherings and benefit activities. More than EUR 130,000 of this amount was allegedly withdrawn in cash and taken to Syria by the suspects.

Conclusions: The terrorism financing threat relating to companies is considered moderately significant/significant (level 2/3).

Money laundering

As highlighted in the latest European Union Serious and Organised Crime Threat Assessment (2021 EU SOCTA)[240] "legal business structures such as companies or other entities are used to facilitate virtually all types of criminal activity with an impact on the EU. Criminals directly control or infiltrate legal business structures in order to facilitate their criminal activities. All types of legal businesses are potentially vulnerable to exploitation by serious and organised crime. More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities. About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level."

One of the factors that might contribute to a higher frequency of misuse of a particular type of legal person is the absence of accurate and up-to-date information on its ownership and management.

According to a joint study of the Financial Action Task Force (FATF) and the Egmont Group, "legal persons, specifically companies, are prominent features of most schemes and structures designed to obscure

[238] IE NRA LPA.
[239] NRA NL.
[240] Europol, 2021 European Union Serious and Organised Crime Threat Assessment (EU SOCTA), 12 April 2021: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

beneficial ownership. […] The separation of legal and natural personalities offered by companies is a key feature influencing this popularity"[241].

Complex structures can also be used to obscure beneficial ownership, avoid taxation obligations, conceal wealth[242], and launder the proceeds of crime. The majority of cases that involved tax evasion, fraudulent investment schemes and fraud also utilized complex structures to conceal beneficial ownership[243]. It has also been reported that "the use of shell companies in complex corporate structures designed to disguise beneficial ownership is a consistent and enduring technique used by criminal groups, corrupt individuals, and complicit professionals. The increased availability of shell companies to foreign nationals, which has been made possible by the growth of global communications and the convergence of international trade markets, has exacerbated this issue"[244].

Front companies can be exploited to launder the proceeds of crime through the integration of illegitimate funds with legitimate income, often hiding the illegitimate funds as cash sales made during the course of business. These funds can then be transferred to the beneficial owner via bank account deposits or payments of false expenses[245].

A front company may be involved in legitimate trading activity. The primary risk indicator is usually the cash-intensive nature of the company – where goods and commodities would be mostly paid for in cash and exported before being re-exported between different countries. In these cases, the services of a complicit bookkeeper or accountant may be used to legitimize criminal cash flows through false invoices, receipts and accounts. Financial statements can also be falsified to account for the cash flows[246].

Finally, offshore companies can also constitute a threat[247], especially when the fact of being incorporated abroad is a threat for transparency by obfuscating the exchange of information. As described above, offshore companies are often lacking real economic activity in the jurisdiction of incorporation. This, together with the high number of intra-affiliated-companies transactions, could increase the risk for such companies of being used as mere vehicles for money laundering purposes.

Front companies Luxembourg[248]
An alleged mafioso was nominated as managing administrator of a small private limited liability company (SARL). This person was nominated without a notarised deed, which means that his name was added in a small statute change after the creation of the SARL; the notary himself was not implied in these changes. When preparing such deeds, notaries check the identity of the beneficial owner.

[241] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 20.
[242] Complex structures are used to prevent being able to identify indirect control of a legal person, in particular in light of the 25% threshold for BO identification of legal persons in the EU.
[243] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 27. See also ES NRA.
[244] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 29. See also ES NRA.
[245] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 29.
[246] IE NRA LPA.
[247] NL NRA on ML (2019); ES NRA.
[248] Case quoted in Luxembourg NRA (case study 15)

Fictitious company turnover[249]
A person involved in cannabis cultivation started a taxi company with 12 taxis with the aim of laundering the criminal proceeds. Private loans and turnover were falsified via the company. The stated turnover did not correspond with the data recorded by the taximeters.

The Netherlands[250]
International company A headquartered in The Netherlands paid corruption funds to a government employee via letter box companies. An international company was registered in an international jurisdiction, with a government employee listed as the beneficial owner but with nominee shareholders and directors. Payments were made via a Dutch bank account of a subsidiary of the international company to an account of the international company in Estonia and via an enterprise registered in Hong Kong, after which these funds were paid into bank accounts in a foreign jurisdiction and from there to a Luxembourg bank account of the international company. Bribes were also paid to charities that were directly associated with government employees. In order to account for the bribes, false invoices were entered in the accounting records.

Multi-national group (within and outside the EU)[251]
Embezzled public funds worth RUB 300 million (Russian rubles) (USD 11 million) were transferred from the account of Company K to the account of Company R. Company R, a Delaware corporation, was owned and managed by the Russian wife of the suspect, a state official. The same day, Company R transferred USD 11 million as a loan to an account of Company A (BVI) held by a Cypriot bank. Company A then transferred more than USD 11 million to the Company D (US) to purchase real estate in France. Company D transferred more than USD 12 million to a French Notaries Bureau. Information from the FIU of Luxembourg showed that one of the US banks acted as a guarantor for the suspect's wife in a transaction to purchase of shares of a French company – and the holder of the real estate. The transaction was conducted via an S.S. company – a French subsidiary of a Luxembourg S.D. SA., incorporated and owned by the same individual. Analysis showed that these two chains were interrelated and the real estate was purchased with the proceeds of public funds embezzled for the benefit of the state official's wife.

Conclusions: The money laundering threat relating to companies is considered very significant (level 4).

[249] NL NRA on ML (2019).
[250] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 33.
[251] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 28.

Vulnerability

Terrorist financing

Criminals may have intentions to exploit these structures for international and domestic terrorist financing purposes. There has been little evidence of their misuse[252]. However, the recent update to FATF/EGMONT report notes that, in practice, trade-based terrorism financing schemes can and do rely on the common trade-based money laundering techniques[253]. Risks of trade-based terrorism financing are likely to materialize as terrorist groups increasingly adopt the operational methods of organised crime groups.

Conclusions: The terrorism financing vulnerability relating to companies is considered moderately significant/significant (level 2/3).

Money laundering

It can be seen that all cases analyzed above involved the use of a company, which indicates that these vehicles are significantly attractive for misuse.

A range of characteristics have been identified which allow companies to be exploited to hide beneficial ownership information. Key techniques used to this purpose can be categorized as follows[254]:

- generating complex ownership and control structures through the use of legal persons and legal arrangements, particularly when established across multiple jurisdictions;
- using individuals and financial instruments to obscure the relationship between the beneficial owner and the asset, including bearer shares, nominees, and professional intermediaries; and
- falsifying activities through the use of false loans, false invoices, and misleading naming conventions, fictitious turnover[255].

Shell companies and front companies feature prominently in most complex structures identified by FIUs and other competent authorities[256].

The use of numerous legal persons or arrangements within a single legal structure, numerous bank accounts and nominee directors, can significantly impair efforts by FIUs, other competent authorities, and financial institutions to identify and verify the beneficial owner. This is further frustrated when legal ownership structures span numerous jurisdictions[257].

Cash-intensive companies, such as catering or retail, nail salons, hairdressers or ice cream parlours, can be misused to provide cover for the source of otherwise inexplicable quantities of cash. In most cases, such businesses are used as a legitimate source of income to facilitate the mixing of illicit funds with legal proceeds[258]. These businesses may be owned by the criminal or by the criminal's straw men. Not only can all business investments be paid for with the criminal cash, but the company turnover can also be falsified.

[252] IE NRA LPA.
[253] FATF/Egmont (December 2020), *Trade-based Money Laundering: Trends and Developments*, p. 33.
[254] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 26; IE NRA LPA; NL NRA on ML (2019); ES NRA.
[255] NL NRA on ML (2019).
[256] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 26.
[257] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 27.
[258] IE NRA LPA, NL NRA on ML (2019).

Criminal cash can be mixed with the legal turnover of the company, after which the total amount is reported to tax authorities as the achieved turnover[259].

Criminals use trade-based money laundering to justify the movement of criminal proceeds through banking channels, for example, via letters of credit and invoices, or through the use of global transactions, often using false documents for the trade of goods and services. It can potentially allow the rapid transfer of large sums camouflaged as a legitimate economic transaction[260].

Law enforcement authorities and FIUs report that although trade-based money laundering schemes require moderate levels of technical expertise and knowledge, they have been frequently used by organized criminal groups because they are generally quite accessible, have low costs and are relatively easy to exploit[261].

The analysis above suggests that where organized criminal groups have connections to a jurisdiction, they may seek to move illicit proceeds to and from that jurisdiction to facilitate offending, often in relation to drug offences.

Conclusions: The money laundering vulnerability relating to companies is considered very significant (level 4).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as moderately significant/significant (2/3), while the level of vulnerability has been assessed as moderately significant / significant (2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as highly significant (4), while the level of vulnerability has been assessed as highly significant (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

In light of the above, the overall level of money laundering risk for companies, from both domestic and international sources, is considered very high.

The overall level of terrorist financing risk for companies, from both domestic and international sources, is considered medium.

Conclusions: the estimated risk level for terrorist financing is MEDIUM and for money laundering VERY HIGH.

[259] NL NRA on ML (2019).
[260] IE NRA LPA.
[261] IE NRA LPA.

Mitigating measures

In light of the above-mentioned threats and vulnerabilities, it is essential to stress that the integrity of the EU financial system depends on the transparency of legal persons.

For this reason, the EU has always been committed to implement an effective AML/CTF framework, specifically targeting the main issues related to companies.

In this context, and going beyond 2012 FATF Recommendations, since 2015 the EU adopted:

- Directive (EU) 2018/843[262], the 5th AMLD (Amendments to the 4th AMLD);
- Regulation (EU) 2015/847 on information on the payer accompanying transfers of funds[263] in order to make fund transfers more transparent and to help law enforcement authorities to track down terrorists and criminals;
- Directive 2018/822/EU[264], which requires intermediaries to submit information on reportable cross-border tax arrangements to their national authorities comes into effect as from 2020.

In particular, Article 30 AMLD provides that:

- Companies should obtain and hold adequate, accurate and current information on the arrangement's beneficial ownership;
- Companies should provide information about their legal owner and the beneficial owner to obliged entities when the obliged entities are taking customer due diligence measures;
- The information mentioned above should be accessible in a timely manner by competent authorities and FIUs;
- The information mentioned above, as adequate, accurate and current, should be held in central register.

The AMLD also obliges Member States to establish effective, proportionate and dissuasive measures or sanctions for breaches of the above obligations.

Based on the information reported by the Member States, the above mentioned obligations have been implemented or are in the process to be implemented.

As risks emanating from legal persons remain high, the AML Package of July 2021 provides for a number of measures aimed at mitigating those risks. In the meantime, Member States and competent authorities should prioritise the following mitigating measure:

- Carry out a risk assessment of ML/TF risks associated with legal persons and regularly review it.
- Ensure that beneficial ownership registers are fully populated and that there are mechanisms in place so that the information they contain is adequate, accurate and up-to-date.

[262] 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.*
[263] 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.*
[264] 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.*

- Provide outreach / training sessions to obliged entities on the identification of beneficial owners and on the detection of discrepancies between the information collected in the context of customer due diligence and the information reported by legal entities to the register of companies' beneficial ownership.
- Conduct thematic inspections on how beneficial ownership identification requirements are implemented by obliged entities.
- Ensure that obliged entities are aware of risks associated with legal persons, particularly in the context of non-face to face business relationships, and when dealing with non-EU legal entities and require that in those cases obliged entities pay particular attention to the corporate structure of the client to ascertain who ultimately owns or controls it.

Last but not least, the Commission has also presented a proposal to combat the use of shell entities in the EU laying down the rules to prevent the misuse of companies for tax purposes and amending Directive 2011/16/EU[265].

[265] COM_2021_565_1_EN_ACT_part1_v7.pdf (europa.eu)

4. High value goods – artefacts and antiquities

Product

High value goods - artefacts and antiquities (high end of the art & antiquities market)

Sector

High value dealers

Description of the risk scenario

Quite a number of EU Member States already include a separate chapter within their National Risk Assessment (NRA) devoted to the art and antiques sector (among others, Finland, France, Germany, …). Their comments ad perceptions, and also those coming from extra-EU States, like Switzerland or the United Kingdom, have been taken into consideration when drafting this assessment.

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[266] at possibly the third or fourth largest category. However there are hardly any statistics showing the actual magnitude of trafficking of artefacts and antiquities, neither on the licit market nor on the illicit market(the specific feature of this illicit trade being that the legal and the illicit trade are sometimes interwoven)[267]. Although cultural goods trafficking is a global phenomenon, there are no comprehensive figures on its global extent. Many crimes remain invisible in the statistics, such as those concerning artefacts and antiquities that have not been previously recorded or inventorised, for example illegally excavated antiquities.

Nevertheless, according to Interpol, the black market in works of art is becoming as lucrative as those for drugs, weapons and counterfeit goods[268].

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[269].

The value of the illegal antiquities traffic is also hard to assess[270] due to its invisible and seamless character[271]. It is estimated that only 30-40 % of antique dealings take place through auction houses where

[266] By the sources consulted and referred to throughout this chapter.
[267] Terrorist financing through the sale of looted artifacts has only been reported outside the EU.
[268] On the other hand, EUROPOL considers it as a limited threat and certainly not comparable to trafficking in drugs, counterfeited goods, or weapons.
[269] 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
[270] 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.
[271] 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.*

the pieces are published in catalogues[272]. The rest occurs through private (thus often unmonitored, and not recorded) transactions[273].

Some studies suggest that 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[274] and has been estimated at $3-6 billion per year[275].

As regards the dimension of the **licit art market**, the Art Basel 2022 report[276] estimates:

- Global sales of art and antiques reached an estimated $65.1 billion, up by 29% from 2020, with values also surpassing pre-pandemic levels of 2019.
- The online market continued to expand in 2021, growing by 7% to reach an estimated $13.3 billion. Online sales accounted for 20% of sales in the art market, down by 5% in share year-on year but still more than double the level of 2019 (9%).
- The US market retained its leading position, shifting up slightly to 43% of worldwide sales by value. Greater China was the second-largest art market with 20%, while the UK slipped back to third place at 17%.
- Outside of the art market's $65.1 billion in turnover, sales of art and collectibles NFTs saw substantial growth in 2021. External sales in these two categories on NFT platforms on the Ethereum, Flow, and Ronin blockchains have grown from $4.6 million in 2019 to $11.1 billion in 2021. The value of sales for art-related NFTs expanded over a hundredfold year-on-year reaching $2.6 billion.

The art market today, especially at the top end, is highly global. For example, a gallery located in Amsterdam might represent and artist from Germany and sell to an American collector. Although China is now one of the leading countries in terms of auction sales, the globalized art world is still centred around the West, with the key cities being New York and London, with Hong Kong coming in third place[277]. Links between the antiquities trade and drug, wildlife and arms trafficking, money laundering and tax evasion and the financing of armed conflicts 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[278].

---

[272] Peter Watson, Sotheby's: The Inside Story, Random House, 1997, cited in Chauncey D. Steele.
[273] Alesia Koush, op. cit., p. 4.
[274] Lisa J. Borodkin, "The Economics of Antiquities looting and a Proposed Legal Alternative", *Columbia Law Review*, No 2, 1995, p. 377-418.
[275] *Ibid.*, p. 377. Estimation by the author.
[276] The Art Market 2022. An Art Basel & UBS Report. Prepared by Dr Clare McAndrew: https://artbasel.com/about/initiatives/the-art-market
[277] Dirty Money, Pretty Art. Fighting Money Laundering in the Age of Art Financialization (May 2020): https://www.veiligondernemenlimburg.nl/content/user_upload/Dirty_Money__Pretty_Art_-_Fighting_Money_Laundering_in_the_Age_of_Art_Financializaton.pdf
[278] Dev Odedra, an independent anti-money laundering and financial crime expert told *Forbes* that art remains an attractive vehicle for those seeking to move money discreetly: *"It's the (almost) perfect mode. It's a bearer instrument* (whoever possesses it can own it), *it can be sent country to country without the watchful eye of regulators* (unlike money in a bank account). *Something about the size of an A3 paper worth millions could be kept at home* (or in a warehouse) *for years."* https://www.forbes.com/sites/daviddawkins/2020/07/30/putins-billionaire-judo-buddy-accused-of-buying-art-to-launder-money-despite-us-sanctions/?sh=3c1bb1424e5f

Art is comparable to a commodity, and as such it can be used in trade-based money laundering to transfer value to others or across borders. In this manner, proceeds of crime can be moved or transferred without using a bank to simply transfer funds that criminals know are monitored for suspicious activity. Here is an example of how art is used for trade-based money laundering: Criminal A sells an inexpensive piece of art to Criminal B but issues an invoice to B for US$1 million. B then wires US$1 million to A and both can then legitimize the money transfer using the invoice[279].

Furthermore, criminals typically enjoy luxury possessions, which can include artwork.

The art market can be attractive for money laundering due to a number of peculiar features:

- Discretion has always been a distinctive feature of the art market.
- Use of intermediaries/proxies for transactions is quite common.
- Art market is intrinsically an international market.
- Due to their peculiar nature, some works of art can reach extremely high prices without raising attention (e.g. paintings, archaeological goods, etc.). Money launders can exploit this feature. Since their main objective is only to convert illicit funds into clean assets they do not follow an economic rationale for transactions, it means that they may boost prices overestimating goods.
- Purchasing a work of art legitimizes cash and converts it into an asset that increases value and can be sold at a later stage.

The impact of COVID-19

Auction houses and art dealers are, like many other sectors, responding to the COVID-19 crisis by shifting operations online. The increased use of digitalised sales platforms has opened up art sales to a greater number of potential buyers across the globe. Thus the effect of COVID-19 has led to heightened risk of abuse of the art market, with the increased use of online platforms and fraudsters seizing the opportunity to exploit businesses through the possible recourse to anonymous transactions.

Threat

Terrorist financing

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

The assessment of the terrorist financing threat posed by the trafficking of looted artefacts and antiques[280] 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[281] 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 of antiquities in countries outside the EU, notably in conflict zones such as Syria,

[279] Deloitte, Art & Finance Report 2019, 6th edition (p. 215): https://www2.deloitte.com/lu/en/pages/art-finance/articles/art-finance-report.html
[280] EU SOCTA 2021: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment
[281] https://blogs.state.gov/stories/2018/06/20/en/tackling-illicit-trafficking-antiquities-and-its-ties-terrorist-financing

and the terrorist organisations that control the territory then imposing taxes on these activities. Terrorist groups are supposed to be involved in granting "licenses" for excavations and facilitating the movement of artefacts out of the origin territories through smuggling routes used for other illicit commodities. For example, 'rather than trading artefacts, Islamic State is earning money from selling digging permits and charging transit fees'[282]. However, terrorists may also sell the products themselves to obtain revenues, as shown by primary evidence collected by the US[283]. and as acknowledged by the United Nations Security Council[284].

Looting of archaeological goods is supposed to be the most used mechanism to generate ill-gotten funds for the financing of terrorism. Crisis areas often include vast territories rich in archaeological heritage that are constantly looted with the aim of collecting valuable artefacts to be smuggled into EU countries with large antiquities markets (e.g. Germany, Belgium, The Netherlands, etc.). US and UAE are also considered regional hubs for illegal antiquities trading.

These goods are provided with fake documents of origin in order to infiltrate the legitimate art market. Considering that these goods have never been recorded anywhere, once they are provided with a false back-story any check about their legitimacy is almost impossible.

It is worth mentioning that the above scenarios have not been confirmed by judicial evidence. Although the smuggling of archaeological goods from crisis zone into the EU has been demonstrated by several investigations, lack of cooperation with source countries has not allowed to collect enough evidence to demonstrate the link between this trafficking and terrorist groups.

The majority of the objects stolen by or with the support of 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 cash requires time to plan, which is not consistent with most terrorist groups' needs to access cash quickly.

Conclusions: 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

[282] Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes, ICSR, 2017.
[283] https://www.justice.gov/usao-dc/pr/united-states-files-complaint-seeking-forfeiture-antiquities-associated-islamic-state
[284] 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'.*

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 moderately significant (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). Also, cases of looting of art and antiques following the invasion of Ukraine are currently being investigated. (level 2).

Money laundering

The art market is attractive for the commission of other proceed-generating offences, e.g. art forgery, art theft, fraud, tax evasion or corruption.

The assessment of the money laundering threat posed by the trafficking of looted artefacts[285] and antiques shows that this risk scenario may be interesting to organised crime groups, as these 'products' can be converted into cash and/or used to launder the proceeds of crime or evade tax. Law enforcement agencies consider that this kind of traffic occurs mostly in Free zones[286] and that this makes it more difficult to measure the extent of the phenomenon. 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).

Similar conclusions appear in a recent study by the US Department of the Treasury[287]. The report finds that while there is some evidence of money laundering risk in the high-value art market, there was limited evidence of terrorist financing risk. It also remarks that the participants most vulnerable to money laundering in the art market are businesses that offer financial services, such as art- collateralized loans, but are not subject to comprehensive anti-money laundering/countering the financing of terrorism (AML/CFT) obligations. Asset-based lending can be used to disguise the original source of funds and provide liquidity to criminals.

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 introduced on the EU territory 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.

[285] We must distinguish between (i) using laundered money to buy art/antiquities that might be potentially of legal provenance, and (ii) trading looted art/antiquities that are with uncertain provenance, in some case "artificially" created provenance.
[286] Free zones are further defined and treated as its own specific sector within this risk analysis.
[287] Treasury Releases Study on Illicit Finance in the High-Value Art Market, February 2022: https://home.treasury.gov/news/press-releases/jy0588

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, a large part of the illicitly traded cultural artefacts worldwide 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. Most obliged entities are not obliged to carry out any record keeping (e.g. on the origin of artefacts or to whom they are sold) and there is no reporting[288]. Law enforcement and 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 EUR 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, in the absence of common criteria/rules of what "acceptable" provenance, 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.

[288] Even if the 5th AMLD introduced a reporting obligation regarding some art market participants and specific transactions.

Further to the two above-mentioned a*d hoc* measures, Regulation 116/2009[289] and Directive 2014/60/EU[290] also apply. Additionally, Regulation (EU) 2019/880[291] of the European Parliament and of the Council Regulation on the introduction and import of cultural goods has been adopted in 2019. It is one of the measures proposed in the framework of Commission's 2016 Action plan for strengthening the fight against terrorist financing and specifically concerns cultural goods created and/or discovered in third countries, and aims to prevent their illicit trade.

As from 28 December 2020, any physical introduction into the customs territory of the European Union of cultural goods originating in third countries is prohibited, when these cultural goods have been exported in breach of the laws and regulations of these countries. Furthermore as from 28 June 2025, at the latest, the import (i.e. their release for free circulation in the internal market or their placement under special customs procedures, other than transit) of specific categories of cultural goods is subject to certain requirements. By that time, a centralised electronic system for the import of cultural goods ('ICG system') will be developed and become operational[292].

Specifically, for the import of certain categories of cultural goods, such as archaeological objects or parts of monuments at least 250 years old, import licences issued by the competent EU Member State authorities will be required regardless the value of the cultural good. For other categories of cultural goods (such as rare collections and specimens of fauna, flora etc. ethnographic objects, paintings, sculptures, manuscripts, old books etc.) that are older than 200 years and have a value of EUR 18,000 or more, an importer statement must be submitted by the holder of the goods. Such an importer statement consists of a declaration that the goods have been lawfully exported from the non-EU country and a standardised document describing the relevant cultural goods.

The submission of applications by operators to competent authorities to obtain an import licence as well as the submission of importer statements are to be carried out via the ISG system. The import licence or the importer statement must be provided to the customs authorities at the time of the submission of the customs declaration. In the case of placing cultural goods under the free zone procedure, the holder of the goods should provide the import licence or the importer statement upon presentation of the goods.

Currently, Regulation (EU) 2019/880[293] applies to those cultural goods which were either created or discovered outside the customs territory of the Union.

Europol is also actively involved in investigations and prosecutions of cultural goods trafficking, for example the yearly multinational PANDORA operations in the framework of the multidisciplinary platform EMPACT[294] which have led to the arrest of 185 people and the recovery of 62.500 looted and stolen objects since 2017.

---

[289] Council Regulation (EC) No 116/2009 of 18 December 2008 on the export of cultural goods (Codified version); *OJ L 39, 10.2.2009, p. 1–7.*

[290] Consolidated text: Directive 2014/60/EU of the European Parliament and of the Council of 15 May 2014 on the return of cultural objects unlawfully removed from the territory of a Member State and amending Regulation (EU) No 1024/2012 (Recast) (Text with EEA relevance); *OJ L 159 28.5.2014, p. 1.*

[291] 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, *OJ L 151, 7.6.2019, p. 1–14.*

[292] The Commission has adopted already two Progress Reports on developing the ICG to the European Parliament and to the Council (1st Progress Report COM(2020)342 and 2nd Progress Report COM(2021)358).

[293] 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, *OJ L 151, 7.6.2019, p. 1–14.*

[294] https://www.europol.europa.eu/newsroom/news/over-18-000-items-seized-and-59-arrests-made-in-operation-targeting-cultural-goods

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 current 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 very significant (level 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 EUR 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. The G20 Culture meeting under the Italian Presidency had as one of its topics the illicit traffic of cultural goods.

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 very significant (level 4).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as significant / very significant (3/4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as moderately significant / very significant (3/4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, terrorist financing and money laundering is HIGH.

Mitigating measures

For the Commission (measures adopted since the previous SNRA):

- On 17 April 2019, Regulation (EU) 2019/880 on the introduction and the import of cultural goods[295] to set out conditions and procedures for the **entry of cultural goods into the customs territory of the Union,** was adopted. The Commission has also carried out a study on 'Improving knowledge about illicit trade in cultural goods in the EU, and the new technologies available to combat it'[296].
- Regulation 2018/1805 on the **mutual recognition of freezing and confiscation orders** (the illicit trafficking of cultural goods is mentioned in Art.3)[297].
- The Commission has also adopted legislation[298] to reinforce the EU framework on preventing the financing of terrorism by increasing the **transparency of cash payments.**

Measures under preparation and recommendations:

- 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.
- The Commission will adopt an action plan tackling trafficking in cultural goods, as announced in the EU Strategy to tackle Organised Crime 2021-2025, adopted in April 2021[299].

[295] 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, *OJ L 151, 7.6.2019, p. 1–14.*
[296] Illicit trade in cultural goods in Europe, 12.07.2019:
https://op.europa.eu/en/publication-detail/-/publication/d79a105a-a6aa-11e9-9d01-01aa75ed71a1
[297] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1805
[298] 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.*
[299] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12735-Fighting-organised-crime-EU-strategy-for-2021-25_en

- The Commission will undertake an evaluation of EU Free zones in 2021-2022. This evaluation will include an assessment of their benefits and costs, including the risk of possible misuse, both in the customs and taxation area.

For Member States:

- Member States should issue guidelines to the art and antiquities sector on how to comply with their AML/CFT obligations. Some jurisdictions (e.g. France, Switzerland, Finland) have already published theirs.
- Member States should implement the existing obligation for signatories of the UNESCO Convention of 1970, enshrined in Article 10 of the UNESCO Convention of 1970, to impose mandatory sales registers for cultural goods, in order to improve traceability of sales within the EU.
- 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.
- In order to better detect cases of trafficking in cultural goods, including those linked to money laundering and terrorism financing activities, Member States should set up specialized police units solely dedicated to crimes related to cultural property in accordance with recommendations from Interpol and the 1970 UNESCO Convention.
- 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.
- Member States should encourage more cooperation between law enforcement and archaeologists, in order to support law enforcement in detecting trafficked cultural goods and determine their provenance.
- 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. (This requirement will be compulsory for certain categories of cultural goods covered by Regulation 2019/880, starting from 2025.)
- 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.
- Considering the cross-border nature of ML/TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML/TF to request support from agencies such as Europol.

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[300] 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[301]

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 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.

The jewellery sector is ideal for laundering money and can be used for both placement and layering. To place incriminated assets, one can simply approach a jewellery store and purchase a ring or a bracelet with cash: paying cash for the jewellery involves changing the asset one holds. Furthermore, there are no fixed market prices in the jewellery sector. This makes it more difficult to accurately assess the market price for jewellery pieces, giving money launderers considerable scope for discretion and manipulation. It should also be considered that jewellery tends to maintain its value and jewellery also tends to be a rather liquid asset[302].

The VAT Directive provides specific rules for transactions related to gold in order to combat tax evasion or avoidance. It allows Member States to include within the taxable amount of a transaction which involves the working of investment gold provided by a customer, the value of that investment gold

[300] Antwerp World Diamond Centre, https://www.awdc.be/

[301] This overall description may be complemented by Teichmann, F.M.J. and Falker, M.-C. (2020), "Money laundering through raw diamonds", *Journal of Money Laundering Control*, Vol. ahead-of-print No. ahead-of-print: https://doi.org/10.1108/JMLC-07-2019-0057

[302] Teichman, F.M.J., "Money Laundering in the jewellery business", *Journal of Money Laundering Control*, Vol. 23 No. 3, 2020; pp. 691-697.

where, by virtue of being worked, the gold loses its status of investment gold. However, this scheme is related only to transactions of investment gold on a regulated gold bullion market, therefore the trade of other kind of gold within a free zone may escape such rules.

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[303].

Conclusions: The level of terrorist financing threat related to the purchase of gold and diamonds is considered as moderately significant (level 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).

Europol Financial Intelligence Public Private Partnership (EFIPPP): in relation to investment fraud, in Boiler rooms schemes, scammers take advantage of the recent decline in asset prices to sell fraudulent investments in gold, silver and other commodities labelled as a safe haven as well as low value stocks or high risk financial products such as derivative instruments and cryptocurrencies. An indicator is: offers misrepresenting value of standard gold bullion coins or promising to provide safe storage for gold.

EFIPPP information: Trade Based Money Laundering is one of the techniques used by Money Laundering Controller Networks.

Money/cash is not directly transferred but transformed into other value (cash, gold, goods, cryptocurrencies, etc.). By means of Trade-Based Money Laundering -TBML-, such as import/ export of goods and Informal Value Transfer Systems -IVTS-, the network transfers funds or an equivalent value payable to a third party in another geographical location.

Generally for illicit trade, the transport of the illicit proceeds in the form of cash, precious metals and jewellery is well known.

[303] As of the 1st of January 2021, the EU Conflict Minerals Regulation covers this area: Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas; *OJ L 130, 19.5.2017, p. 1–20.*
The EU Conflict Minerals regulation means that selected EU importers of the respective minerals (also referred to as '3TG') need to comply with, and report on, supply chain due diligence obligations if the minerals originate even potentially) from conflict-affected and high-risk areas.

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 EUR 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 EUR 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[304] 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.

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 EUR 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.

[304] 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

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 EUR 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as very significant (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔ 2,6 – 3,5 Significant HIGH

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔ 2,6 – 3,5 Significant HIGH

Conclusions: estimated risk level for both terrorist financing and money laundering is HIGH.

Mitigating measures

For the Commission:

- Under the new **Cash Controls Regulation**, the definition of cash has been extended to cover not only coins, banknotes and bearer negotiable instruments, but also commodities used as highly-liquid stores of value, such as gold (i.e. coins with a gold content of at least 90 % and bullion such as bars, nuggets or clumps with a gold content of at least 99,5 %).
- 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.

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.
- Considering the cross-border nature of ML/TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML/TF to request support from agencies such as Europol.

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).

6. High value assets – other than precious metals and stones

Product

High value assets – other than precious metals and stones[305]

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.

A study by the European Parliament's PANA Committee[306] revealed that, according to EUROPOL, 388 out of the 3,469 entries appearing in the so-called Panama papers were connected to VAT fraud operations[307]. Fighting large-scale VAT fraud implies tackling the money laundering processes of fraudsters as well. According to another EU study[308], 21 cases of EU VAT fraud between 2004 and 2010 involved organised crime, with the proceeds potentially being used to finance other types of crime, such as drug trafficking, trafficking in human beings, identity fraud, alcohol smuggling and counterfeiting.

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

[305] We refer in general to our previous analysis on weaknesses from a predicate offense perspective as regards Free zones on art and antiquities as this analysis is also relevant for the current sector of high value assets. The Commission's Evaluation of Free zones as a mitigating measure is also relevant.
[306] Public Sector Reform: How the EU budget is used to encourage it: https://www.econstor.eu/bitstream/10419/147039/1/869811940.pdf
[307] VAT fraud is a horizontal issue, and not actually linked to any commodity in particular.
[308] How does organised crime misuse EU funds: https://www.europarl.europa.eu/meetdocs/2009_2014/documents/cont/dv/crime_misuse_/crime_misuse_en.pdf

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 trade-based money laundering. 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.

EFIPPP information: In relation to the traffic of human beings, organised crime groups send cash/invest the illegal profits in the country of origin, using cash couriers and money service brokers (Western Union, MoneyGram) and / or invested in real estate, luxury vehicles and cash intensive businesses

In relation to corruption and bribery, straw men are used to obfuscate the beneficial owner of a luxurious asset bought with the bribery funds.

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.

On a related note, according to the ECA and Europol, the most damaging VAT frauds are committed by organised crime groups (OCGs) through missing trader intra-community (MTIC) schemes[309]. They benefit from their international criminal structures and connections to establish efficient MTIC schemes to extort money from national budgets. The ECA and Europol estimate that EUR 40-60 billion of the annual VAT revenue losses are caused by organised crime groups and that 2 % of those groups are behind 80 % of the MTIC fraud. The proceeds of MTIC fraud are usually reinvested in new criminal activities or laundered[310].

[309] Missing trader intra-community (MTIC) fraud is the theft of value-added tax (VAT) from a government by organised crime groups.

[310] See also the Strategic Meeting on VAT Fraud organised of 28 March 2011 by Europol under Coordinating Committee in the area of police and judicial cooperation in criminal matters (CATS):
https://data.consilium.europa.eu/doc/document/ST%2011570%202011%20INIT/EN/pdf
The 2013 EU Serious and Organised Crime Threat Assessment (SOCTA) also identified MTIC as one of the top priorities for the fight against organised crime groups (https://www.europol.europa.eu/socta-report) and was followed in the EMPACT initiative (https://ec.europa.eu/home-affairs/policies/law-enforcement-cooperation/operational-cooperation/empact-fighting-crime-together_en).

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 realy 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 EUR 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.

As regard cooperation between Europol and Member States tax authorities they can now exchange some information referring to VAT fraud under certain conditions pursuant to Regulation (EU) No 904/2010 on administrative cooperation and fighting fraud in the field of VAT[311].

[311] Regulation (EU) No 904/2010 as amended in 2018 foresee that Eurofisc (a network of anti-fraud experts of the Member States) and Europol can exchange VAT fraud related information under certain conditions.

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).

Risk level

As regards **terrorist financing**, the levels of threat and vulnerability have been assessed as non-relevant (0).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant (3).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is NON-RELEVANT and for money laundering HIGH.

Mitigating measures

For the Commission:

- The Commission has looked at the potential impact of cash payment restrictions and has published a report on the subject[312]. 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.

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.

[312] 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/transparency/documents-register/detail?ref=COM(2018)483&lang=en

7. Couriers in precious metals and stones

Product

Gold and other precious metals

Sector

Shipping precious metals and stones is usually prohibited by most courier companies. Depending on how valuable the items are, some companies may allow shipping them under specific conditions and upon signing relevant agreements.

Also, independent individuals.

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 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 Controls Regulation entered into application on 3 June 2021, gold was not included in the definition of cash for which a cash declaration was obligatory at the EU's external borders in case its value was equal or more than EUR 10 000. After that date, the following changes apply:

1) The definition of 'cash' in the Cash Controls Regulation is now extended and includes the following:

- Banknotes and coins (including currency now out of general circulation but that can still be exchanged in a financial institution or central bank),
- Bearer negotiable instruments such as cheques, travellers' cheques, promissory notes and money orders,
- Gold coins with a gold content of at least 90 %,
- Gold bars, nuggets or clumps with a gold content of at least 99.5 %.

2) Customs authorities may also now request that a cash disclosure declaration be lodged when they detect EUR 10 000 or more in cash (as included in the new definition), being sent by post, freight or courier (unaccompanied cash). If requested, this declaration should be made within 30 days by the recipient, sender or by an appointed representative of the two.

3) The new rules also authorise customs authorities to act on amounts lower than EUR 10 000 when there are indications that the cash is linked to criminal activity.

Conclusions: Still 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. 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

Assets such as gold/precious stones 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: Still 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as significant (2), while the level of vulnerability has been assessed as very significant (4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
➔	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as very significant (4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is HIGH and for money laundering VERY HIGH.

Mitigating measures

As recommended by the SNRA 2017 the Commission has adopted a new Cash Controls 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

Real estate is as attractive to criminals as it is to any investor (prices being generally stable and likely to appreciate over time) and is also functional (the property can be used as a second home or rented out, generating income). Real estate also provides a veneer of respectability, legitimacy and normality.

Although the exact scale of illegal activity in the sector is difficult to estimate, according to a 2019 report by the European Parliament[313], the share of real estate in criminal assets confiscated, which can be used as an indicator as to how much money is laundered through real estate, was estimated at 30% between 2011 and 2013. It was also noted by a 2021 Europol report[314] looking at organized crime trends in the European Union that most criminal groups and networks (68%) use money laundering methods, such as investing in property, to try to legitimize or hide their illicit proceeds. A 2018 report on real estate money-laundering vulnerability provides an assessment of the magnitude of foreign money of unclear origin laundered into German real estate in 2017 (about EUR 30 billion, with 15 to 30% of criminal proceeds having been invested in real estate) and a description of the phenomenon[315]. After tightening reporting requirements regarding real estate transactions, Germany witnessed a 100-fold increase in reports by notaries between 2019 and 2020[316]. An author specialized in the assessment of the illicit economy, A.F. Steinko[317], estimates the relevance of money laundered through real estate as high as 80% of the total of criminal proceedings. Figures may vary, but even the lower estimate underlines the significance of the problem.

Common methods used by criminals in ML/TF schemes involve the use of complex loans or credit finance, intermediation via professionals, the use of corporate vehicles, manipulation of the appraisal or valuation of a property, the use of monetary instruments such as cash or cheques, the use of mortgage schemes or the use of properties to conceal money generated by illegal activities[318]. It is also common for criminals to invest high amounts of money (ill-gotten funds) to rebuild or renovate real estates. Afterwards, they could use them for their own benefit (houses, apartments or business offices) or they could sell those real estates with a much higher price than they purchased and justifying the income.

Beneficial ownership[319] appears difficult to be ascertained, given that the structures put in place for the acquisition or properties may be incredibly sophisticated. The Pandora Papers show examples of the

[313] https://www.europarl.europa.eu/cmsdata/161094/7%20-%2001%20EPRS_Understanding%20money%20laundering%20through%20real%20estate%20transactions.pdf
[314] Europol, 2021 European Union Serious and Organised Crime Threat Assessment (EU SOCTA), 12 April 2021: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crimethreat-assessment
[315] https://www.dw.com/en/german-real-estate-market-a-hotbed-of-money-laundering-transparency-reports/a-46637937
[316] https://www.zoll.de/SharedDocs/Pressemitteilungen/DE/Bargeld/2021/z85_fiu_jahresbericht.html?nn=290366
[317] A.F. Steinko, *La economía ilícita en España*, Alianza Editorial, 2021, p. 345.
[318] FAFT/OECD, *Money laundering and terrorist financing through the real estate sector*, 2007.
[319] The current EU AML framework does not include identifying BO owners of legal persons/arrangements holding real estate. This is particularly problematic if the legal person/arrangement is non-EU and will therefore not be subject to BO register requirements anywhere in the EU. The 2021 package seeks to address this issue.

fiscal and legal engineering put in place aimed at concealing the origin of the money[320]: In some cases the beneficial owner can be identified, in other cases it is extremely complicated, especially when there is an interposition of companies. Money laundering through the real estate sector does not necessarily have to be expensive, but can actually be quite profitable. By making certain cash payments, criminals often succeed in circumventing tax laws and, thereby, become more profitable than legitimate operators in the real estate business[321].

On a directly related issue, the recent Commission study on Monitoring offshore wealth hidden in international financial centres[322] has estimated that EUR 1.4 trillion is held in offshore real estate by EU residents. Through interviews with relevant stakeholders, the study confirmed that tax evasion using the real estate sector is cited as a significant problem in many Member States. The use of shell companies like foundations and private limited liability companies to conceal beneficial ownership information, the use of cash to purchase real estate, purchasing real estate at lower than market values, as well using financial instruments like back-to-back loans, have been cited as methods for both money laundering and tax evasion purposes. Whilst information on the ownership of real estate is exchanged between Member States under Directive 2011/16/EU on Administrative Cooperation in Direct Taxation[323], this depends on information being available in the first place in the Member State where the property is located. Secondly, the information that is available, for example in land and property registers, does not contain information on beneficial ownership of legal persons and arrangements holding real estate.

The impact of COVID-19

The Covid-19 pandemic has undermined demand in the European markets and that has caught the eye of international buyers, including those hoping to launder dirty money. It is also possible sellers and their agents have paid less attention to due diligence in their eagerness to complete deals. Commercial real estate sellers, in particular, have faced pressure to transact quickly, as the impacts of Covid-19 have rocked the economy. Both EUROPOL and the FATF highlighted early on in the ongoing crisis, that criminals may seek to invest in real estate and that the real estate and construction sectors will become even more attractive for money laundering both in terms of investment and as a justification for the movement of funds[324].

Threat

Terrorist financing

For the purpose of this Supranational Risk Assessment the terrorist financing threat related to real estate investments would be no different from the threat relating to organised crime and money laundering. Therefore, it is not being considered as different to the threat of abuse for the purpose of money laundering.

[320] Pandora papers, France: https://remonews.com/franceeng/luxury-real-estate-on-the-french-riviera-a-money-laundering-paradise/

[321] Teichmann, F.M.J. (2018), "Real estate money laundering in Austria, Germany, Liechtenstein and Switzerland", *Journal of Money Laundering Control*, Vol. 21 No. 3, 2018, pp. 370-375, DOI 10.1108/JMLC-09-2017-0043

[322] https://op.europa.eu/en/publication-detail/-/publication/0f2b8b13-f65f-11eb-9037-01aa75ed71a1/language-en/format-PDF/source-242666547

[323] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC; *OJ L 64, 11.3.2011, p. 1–12.*

[324] https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu , and https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

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.

Europol Financial Intelligence Public Private Partnership (EFIPPP) information, stemming from EFIPPP typology reports:

ML through real estate is related to various crime types:

Trafficking in Human Beings (THB): Organised Crime Groups involved in THB sent cash/invest illegal profits in the country of origin: using cash couriers and Money Service Businesses (Western Union, MoneyGram) and / or investing in real estate, luxury vehicles and cash intensive businesses.

Investment fraud: buy low, sell high schemes targeting commodities and real estate, cryptocurrencies or complex derivative products.

Misuse of public funds: the customer wants to have power of attorney for 3rd parties, i.e. a signal for a straw borrower scheme (individuals with good credit record are hired by criminals to act as a front person for borrowing money or buying certain movable and immovable properties).

Corruption and bribery: use of straw men to obfuscate the beneficial owner of a luxurious bought with the bribery funds.

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 money laundering 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

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. Cash is still intensively used by construction companies and freelance professionals. They use cash to buy materials (VAT fraud) but also to pay workers (non-declare working hours). Illicit cash is used not only to buy real estates but also for renovation or for building purposes.

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)[325], and therefore increasing the risk exposure. Real estate activities may be based on financial flows coming from outside the EU[326] and high-risk customers, such as politically exposed persons. As already mentioned, cooperation with involved third countries is in many cases suboptimal and hampering the possibilities to reduce the risk of ML/TF through real estate.

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.

The sector is 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

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.

[325] 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 should increase the chance of detecting anti-money laundering activities.

[326] As noted above EU property held by non-EU companies will not be subject to BO identification rules under EU AML framework.

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'[327].

Practices in the sector differ with efforts being made by representative professional associations to promote awareness and good practice examples for their members.

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 very significant (level 4).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as very significant (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant/very significant (level 4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for both, terrorist financing and money laundering is VERY HIGH.

Mitigating measures

Anonymity represents the most basic and pernicious AML problem in general. In real estate purchases, it can be abused in the same way as anonymity in financial services. Therefore, efforts must be directed towards collecting beneficial ownership information guaranteeing its transparency.

[327] An intra budgetary financial arrangement in which both payments and receipts occur within the same trust fund group.

For the Commission:

Following changes introduced by Directive (EU) 2018/843[328] ("AMLD5"), information on real estate ownership must be available for national anti-money laundering and countering the financing of terrorism (AML/CFT) authorities. Article 32b(1) of AMLD requires Member States to provide Financial Intelligence Units (FIUs) and competent authorities with access to information which allows the identification in a timely manner of any natural or legal persons owning real estate, including through registers or electronic data retrieval systems where such registers or systems are available.

As published by the European Commission in its recent report on real estate registers[329], a way to guarantee the necessary transparency on beneficial ownership information would be that of following those successful initiatives concerning interconnection of national land registers, which could pave the way for potential legislative actions.

For competent authorities:

- 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.
- On-site inspections commensurate to the population of the real estate representatives in the Member State's territory and assessing inherent risks like whether the real estate sector is regulated or not, whether a legal representative like a notaris is involved in the transaction, or whether real estate members are required to be authorised to deal in real estate transactions.

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).
- A low threshold of payment in cash should be implemented for purchases of assets (reals estate).
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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'[330], 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).

[328] 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, *OJ L156, 19.6.2018, p. 43-74.*

[329] "Report from the Commission to the European Parliament and the Council assessing the necessity and proportionality of harmonising the information included in the real estate registers and assessing the need for the interconnection of those registers", Brussels 2021, COM(2022) 87 final.

[330] https://networkcultures.org/wp-content/uploads/2019/03/Flying-Money-Conference-reader-2018.pdf

9. Services provided by accountants, auditors, advisors and tax advisors

Product

Services provided by accountants, auditors, advisors and tax advisors

Sector

External accountants, auditors, advisors and tax advisors

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

Accountants, auditors, advisors and tax advisors work in diverse capacities and sectors: as members of the staff of the company on which they provide their services or as self-employed or consultant company's staff in accountancy firms, SMEs, large companies, governments, non-profit organisations, education, etc.

In the EU, the profession is bound by AML/CFT requirements provided by specific EU legislation.

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 sound governance, ethics and sustainability. The organisations report these measurements to the outside world so e.g. investors can base their decisions on the organisation's performance. In some instance, they can provide additional services (see advisors below).
- Auditors[331] provide a legally mandated check of the financial accounts of large and medium--sized undertakings and form an opinion on them.
- Advisors: Many organisations rely on the professional 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.

Nevertheless, there are relevant differences between Member States in terms of how accountants/tax advisors are organised and regulated. One or more professions in these sectors are regulated in 18 Member States, either:

[331] For further information on "Role of audit" in the EU: https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/auditing-companies-financial-statements_en

- by way of reserved activities and protected titles[332];
- by reserved activities[333]; or
- by protecting the professional title only[334].

In nine Member States[335], none of the professions in the field are directly regulated. Other Member States generally justify regulating the sector by the role tax advisers/accountants play in all tax systems in assisting consumers, companies and taxpayers in meeting their tax obligations.

Moreover:

- In seven countries[336], 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 appeal procedure.
- In six countries[337], 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 four countries[338], tax advisors may also represent their clients in criminal tax matters (although that does not take place in practice in the Czech Republic and Croatia).
- In six countries[339], 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) that sets out the framework for all statutory audits, strengthens public oversight of the audit profession and improves cooperation between competent authorities in the EU.

Moreover, the Audit Regulation (537/2014/EU) 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

[332] AT, BE, HR, FR, DE, EL, IT, LU, MT, PL, PT, RO and SK.
[333] BU, CZ, HU and IE.
[334] NL.
[335] CY, DE, EE, FI, LT, LV, SI, ES and SE.
[336] BE, ES, EL, IE, PT, RO and SK.
[337] FI, IT, LV, LU, NL and PL.
[338] AT, CZ, DE and HR.
[339] AT, DE, FI, LV, NL and PL.

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 advisors, albeit with a moderate level of involvement of the professionals themselves, with the aim to, as an example:

- create and/or manage trusts and companies;
- identifying people and business struggling financially in order to exploit them;
- arrange fake accountancy/budget to deceive investors, e.g. banks or business partners;
- arrange over or under-invoicing or false declarations for import/export goods;
- undertake litigations;
- provide false assurances and/or guarantees;
- misuse client accounts;
- purchase real estate;
- provide assistance with tax compliance.

Moreover, experts in these fields may be involved in money laundering schemes by:

- providing straw men to manage companies, and
- hosting fake companies headquarters, offices.

Accountants or advisors may offer their services/expertise in helping to creating or promoting "opaque structures", often set up in multiple jurisdictions including offshore centres, 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.

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 legal activities**,** risk of misuse by or active collaboration with organised crime groups is a money laundering threat for accountants, auditors, advisors and tax advisors. These experts may be unwittingly involved in the money laundering but may also be complicit or wilfully negligent in conducting their customer due diligence obligations.

Tax advisors are often used by organised crime groups for setting up corporate schemes that are unnecessarily and unjustifiably complex multi-tiered entities (i.e., corporate schemes composed by

companies which management and ownership rights are in turn held by other companies, often located in a foreign jurisdiction(s), and in particular in offshore centres). Tax advisors' services might be considered instrumental for money laundering schemes because they can combine legitimate tax optimisation practices with illegal activities. Access to tax advisors' services is legitimate and even desirable, even for medium-sized companies. At the same time, sometimes, tax advisors are part of the organised criminal groups and constitute the respectable façade that criminals use to enter into contacts with lawful investors and business' partners and exploit them.

Most of the services provided by these professionals are genuine and used for legitimate purposes. However, they can also support or be instrumental for money laundering schemes, e.g. tax evasion schemes, fraudulent trading, false invoices or declarations for import and export activities, fraudulent bankruptcy, usury, corruption of civil servants.

The involvement of the experts of these sectors might vary. They can just provide services for a specific operation thus giving respectability to that operation or provide their professional services helping in circumventing rules. Moreover, they can have a more in-depth involvement supporting or organising the money laundering schemes.

Professionals in these sectors might be involved pretending to be the beneficial owner(s) of a company and yet, over the course of the business relationship, appear to be acting on the instruction of additional, undeclared parties.

Auditors could be complicit or wilfully negligent while certifying the financial compliance of accountancies and budgets which are then used for misappropriation or wrongful retention of funds.

Professionals in these areas are among the actors most misused by organised crime groups to launder criminal proceeds; this is due to the types of services that they can provide to their clients and their sector of expertise. They can use financial engineering techniques and set up corporate structures, involving not cooperative jurisdictions, fabricating accounting systems, providing bookkeeping services, preparing financial statements or fiscal declarations, reporting false information, acting as insolvency administrator and providing general accounting and tax advice. These services are used by organised crime groups to disguise their identity, to commit predicate offences and laundering the proceeds of these crimes.

Conclusions: Services provided by advisors and tax advisors, auditors and accountants are often used in money laundering schemes disguised under legitimate services. 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).

CASE STUDY 1[340] (IT)

Through AML investigations on a professional office providing services to companies, scrutiny of balance sheet and additional documents, it came up that its client (a joint venture company) was registered in the Member State only few weeks before a large investment of 8 million euros was made in the national real estate sector. The events following the investment were even more suspicious considering that the acquired hotel was abandoned, despite the high potential value of the property in that period (due to international fairs going on in the meantime in the city).

The main facts discovered by national competent authorities are the following:

- The accountant received a mandate to constitute a new company (NewCo) for the real estate acquisition from two companies (X and Y) established in two other Member States;
- The acquisition was funded by loan received from a foreign company located in a low tax jurisdiction;
- Companies X and Y received a mandate to start the whole operations by a foreign trust company which was never identified by the accountant (in breach of his CDD obligations).

[340] Member State's law enforcement information.

CASE STUDY 2 (IT)[341]
In the course of an inspective activity against a trust company established in a Member State, the attention of the investigation focused on the existence of a trustee mandate in the name of a foreign company, for which there was no specification of the ownership nor the reasons for acquiring a well-known national transport company, the shares of which were held by the partners.

The suspicion was that the trust company may have served the only purpose of being a "screen" to transfer funds, illegally generated and concealed abroad, to the Member State. This led to more thorough investigations, allowing to identify approximately 160 permanent accounts related, for different reasons, to the mentioned physical and/or juridical persons. A subsequent examination of the documents obtained enabled to identify the beneficial owner of the foreign company, which in turn allowed to link the investigated persons to the considerable financial assets that had been fraudulently transferred abroad and used to purchase the national transport company.

CASE STUDY 3[342] **(NL)**
A criminal investigation into a Member State's TCSP was instigated on account of the systematic failure to notify unusual transactions and money laundering. This was presumed to involve the facilitation of fake transactions on behalf of foreign clients to ensure, for example, the assets or property of those clients were scarcely taxed, or funds parked were transferred by means of fake transactions to another jurisdiction. This was carried out by means of complicated well-considered structures with companies and trusts in various countries for which instructions were given by a financial service provider and were also discussed in this way by the suspect with the local civil-law notary. National entities were part of these complicated structures. The same applied for the national foundations registered at an international address. The structure sometimes consisted of eight different entities, in various countries. The suspect reportedly did not know in several cases the identity of the actual beneficiaries of the companies that he incorporated).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability 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. 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

Often, accountants, advisors and in particular tax advisors might be involved in the creation or exploitation of complex transactions or financial structures requiring high professional tax or

[341] Member State's law enforcement information.
[342] FAFT and Egmont Group (July 2018), *Concealment of Beneficial Ownership*, p. 73.

accountancy related competences. These activities are a viable solution for high-risk customers (such as politically exposed persons) or to complex corporate structures which might benefit from "opaque" structures in order to hide the beneficial ownership. These sectors of activity are often very profitable and thus require specialised expertise as instrumental for achieving their core business, either legal or illegal.

b) risk awareness

Auditors, advisors and tax advisors are required to comply with strict ethical standards and professional rules often adopted at international level. Standards and rules should safeguard these experts from money laundering and terrorist financing risks. However, these sectors are permeable to organised crime groups or criminals in general; this is coupled with the weakness of some sectoral supervisory bodies which are not properly equipped to prevent and detect the abuse of the system.

These sectors, as well as accountants, benefit from a strong organisational framework at EU level. For instance, "Accountancy Europe" unites 50 professional organisations from 35 countries that represent close to one million professional accountants, auditors, and advisors and is active in the areas of sustainable finance, SMEs, tax, reporting and audit.

The "Association of Law Enforcement Forensic Accountants (ALEFA) is an unincorporated association of forensic accountants who work with law enforcement agencies and civil, non-conviction based asset recovery agencies. It was established to develop the quality and reach of forensic accountancy throughout law enforcement agencies so as to better assist the Courts, victims, witnesses, suspects, defendants and their legal representatives in relation to alleged fraud, fiscal, financial and serious organised crime.

The "European Accounting Association (EAA)", is an academic association that supports high-quality accounting research, teaching and knowledge exchange with practice by providing a platform that enables accounting academics to develop themselves and benefit society through their activities.

The "European Federation of Accountants and Auditors for SMEs (EFAA)" is an organisation for national accountants and auditors' organisations which has 12 members throughout Europe representing over 350,000 accountants, auditors and tax advisors.

The "Confédération Fiscale Européenne, Tax Advisers Europe" is an association representing European tax advisers which brings together 33 national organisations from 26 European countries, representing more than 200,000 tax advisers.

The role of these organisations is to disseminate knowledge about relevant legislation applicable at their specific sectors at national and European level and, with regard to the specific subject of this document, to promote awareness on tasks and obligations that their associated have to comply with in regard to money laundering legislation.

With regard to the auditors, the current rules were adopted in April 2014 in the aftermath of the financial crisis. They aim to improve statutory audits in the EU by reinforcing auditors' independence and their professional scepticism towards the management of the audited company. In 2016, a new framework for co-operation between national audit oversight bodies at EU level was created, i.e. the CEAOB: Committee of European Audit Oversight bodies. Its role is to strengthen EU-wide audit oversight[343]. A particular focus is given to public interest entities (PIEs).

The CEAOB is composed of representatives of:

[343] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/committee-european-auditing-oversight-bodies_en

- the national audit oversight bodies of the EU;
- the European Securities and Markets Authority (ESMA).

Representatives of the national audit authorities of the European Economic Area also participate. The European Banking Authority (EBA) and the European Insurance and Occupational Pensions Authority (EIOPA) are observers.

As remarked by the audit regulation, "good audit quality contributes to the orderly functioning of markets by enhancing the integrity and efficiency of financial statements. Thus, statutory auditors fulfil a particularly important societal role." Accountants, auditors and tax advisors usually pretend not being adequately aware of the importance of their role and the risks opaque structures potentially create.

c) legal framework and controls

Accountants, auditors, 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.

Services of accountants, auditors, advisors and tax advisors could be required in many phases of the life of a corporation or financial structure, from its conception to its bankruptcy. Opaque structures can be created in many jurisdictions, including in offshore centres, with different legal frameworks which makes expertise of these professionals even more attractive. Sometimes these professionals have a long-term business relationships with their client/employer that enhance the capacity to identify unusual transactions or behaviour. Nevertheless, sometimes, services from these experts are required for a one-off or sporadic activities/transactions that reduce the capacity of the professionals to detect the possible opaque nature of the operation/transaction and thus prepare a suspicious transaction report. Experts in these sectors, mainly accountants, advisors and tax advisors, often justify the low numbers of reporting by the fact that they have access to the information the client/employer put at their disposal and have not a full control of the activity on which they are required to provide expertise. Frauds are usually concealed behind formally irreproachable transactions/operations, being the essence of the fraud, and thus to detect a suspicious behaviour is not always simple. Nevertheless, professional scepticism would enhance the possibility for auditors, accountants and tax advisors to detect possible unusual or suspicious transactions/operations increasing their suspicious transaction reports.

Conclusions: Accountants, auditors, advisors, and tax advisors are well organised. However, they may not have access to all information regarding the operation/transaction on which their expertise is requires, and this represent a 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 significant (level 3).

Risk level

As regards **Advisors and Tax Advisors**, the level of threat has been assessed as very significant (4), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **Auditors and Accountants**, the level of threat has been assessed as significant (3), and the level of vulnerability has also been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing/money laundering is HIGH for Advisors and Tax Advisors and HIGH for Auditors and Accountants.

Mitigating measures

For the Commission:

Directive (EU) 2015/849, as amended by Directive (EU) 2018/843, has clarified the applicability of AML provisions with regard to external auditors, accountants and tax advisors: its provisions apply to any other person that provides material aid, assistance or advice on tax matters as their principal business or professional activity.

Also on beneficial ownership, the Directive has clarified the AML legislation in force: corporate entities and trust are required to hold information regarding their beneficial owner and make it accessible to competent authorities and Financial Intelligence Units. Beneficial owners are themselves required to make available to corporate entities the information the latter need to comply with the legal provisions. Corporate entities and trusts have to provide this information to their accountants.

Effective, proportionate and dissuasive measures or sanctions are applied in cases of noncompliance with these rules.

In 2020 the Directive 2018/822/EU entered into force; it requires intermediaries to submit information on reportable cross-border tax arrangements[344] to their national authorities.

The Commission is conducting transposition checks on how the directives have been implemented at national level and in particular, for what is relevant for the accountants, auditors, advisors and tax advisors, 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
- 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.

For the 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

344 https://ec.europa.eu/taxation_customs/taxation-1/tax-co-operation-and-control/general-overview/enhanced-administrative-cooperation-field-direct-taxation_en

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 them immediately and unfiltered to the financial intelligence units. Self-regulatory bodies should draw up annual statistics on the number of reports filed to the financial intelligence units and assess their consistency with the risk exposure of the sector.

- On-site inspections should be carried out on a risk-sensitive basis following an AML/CFT risk assessment of their supervised population. To this end, supervisors should have a clear understanding of the services provided by the legal professionals and risks associated with them.

For Member States:

- Member States should provide guidance on typologies and risk factors arising from transactions involving external accountants and tax advisors.
- In line with the FATF standards, Member States should ensure that when supervision is performed by self-regulatory bodies, they are overseen, for AML/CFT purposes, by a public authority.
- Self-regulatory bodies should intensify inspections, whilst also strengthening the focus on AML/CFT aspects of their checks and ensure that supervision is risk-based.
- Member States should provide guidance on implementing the legal privilege — defining legal services subject to legal privilege and other services not subject to legal privilege. This would improve external auditors, external accountants and tax advisors awareness on how to interpret and apply the legal privilege.

10. Services from notaries and other independent legal professionals

Product

Services from legal professionals

Sector

Independent legal professionals, lawyers, notaries

Description of the sector and risk scenario

All Member States regulate the profession of lawyers, and two EU-level Directives facilitate the provision of services by lawyers across borders (Directive 98/5/EC and Directive 77/249/EEC). Beyond assisting in the administration of justice by representing their clients and allowing them to exercise the right of defense, lawyers provide additional legal services to ascertain the position of their clients as well as services that do not involve legal counselling per se, but are rather of intermediation, counselling and representation in activities of their clients. Many Member States allow a wide range of legal forms through which lawyer can exercise their profession, although some are excluded. Ordinary partnerships are generally allowed and in many Member States professional services can also be provided under the form of a professional company. The possibility to set up a law firm under a specific legal form is strongly linked to shareholding and voting rights requirements. A vast majority of Member States require all the shares to be held by lawyers.

The establishment of new providers of services using algorithms and machine learning solutions who are not themselves legal professionals has given rise to debates on what constitutes legal advice in areas such as the provision of online legal consultations, debt collection and automated drafting of legal documents. At the same time these developments have sparked demand by the legal profession to adapt the regulatory framework to facilitate the adoption of such legal tech solutions.[345]

The profession of notary is not common to all legal tradition of the Member States. A notarial system exists in 22 of the 27 EU Member States (exceptions are Cyprus, Denmark, Finland, Ireland and Sweden). In these countries, the role of the notary is that of a public function holder, tasked with the duty to confer authenticity on the legal instruments they establish for their clients. The notary is responsible for both the content and the form of the instrument. Furthermore, authenticating the instrument requires an impartial role carried out in full respect of the law. Notaries also provide legal advice to their clients, whether in the context of estate planning, succession and asset transfer. Notaries may also have the exclusive competence to draw up legal instruments incorporating and modifying companies, certifying their activity, etc. They may also act as mediators, conciliators or arbitrators.

In the context of the activities performed by lawyers, notaries and other legal professions, they may be exposed to money laundering and terrorist financing risks as regards:

- misuse of client accounts;
- purchase of real state;
- creation of trusts and companies/ management of trusts and companies; or
- undertaking certain litigation.

In addition, there may be situations where legal professions become involved in money laundering schemes by helping create complex chains of legal vehicles, whether in the form of legal persons or

[345] COM(2021) 385 final.

legal arrangements, which conceal the identity of the beneficial owner, including 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 generally requires the services of professionals with dedicated expertise.

Threat

Terrorist financing

The assessment of the terrorist financing threat related to 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 as schemes are similar in nature. This is justified by the fact that terrorists have been known for years to use typical money laundering schemes such as the resort to shell companies or real estate transactions to finance their activities too. 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 services provided by legal professionals has some features in common with services provided by accountants, auditors and tax advisors.

As for all other legal activities, risk of misuse by organised criminal groups is a money laundering threat for lawyers and notaries. These professionals may be unwittingly involved in the money laundering but may also be complicit or negligent in conducting their customer due diligence obligations. The low number of suspicious transaction reports filed by lawyers across the EU, despite the significant risk exposure of the sector in a number of Member States, highlights issues with the implementation of AML/CFT requirements. This is to a lesser extent the case for notaries, who appear to report on average a higher number of suspicions to Financial Intelligence Units.

Law enforcement agencies report that organised crime groups frequently use services provided by legal professionals 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. Such risks are increased by the post-pandemic sector as public funding is injected in the economy to support new activities. 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 become involved in the facilitation of 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 be 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.

Given the very few suspicions reported by lawyers to financial intelligence units, extrapolating useful case studies to exemplify ML/TF threats is difficult. In fact, most cases reported in typologies regarding lawyers or appearing in revelations by investigative journalists refer to situations where the lawyers themselves were found to be actively facilitating money laundering. These typologies confirm nonetheless that risks exists and are very significant.

As regards notaries, exposure to risk materialises both in the provision of advice and in the authentication of instruments. A particularly exposed sector is that of real estate, which generally involves the services of one or more notaries, but for which the notaries might not have the full picture of the transaction and involved parties that would enable them to obtain a holistic view of the risks involved and form a suspicion. Other risk situations involve the certification of a person's status and identity, or the opening of safe deposit boxes.

Case study - Luxembourg[346]
An alleged member of an organised crime group was nominated as managing administrator of a small private limited liability company, without a notarised deed. The notary himself was not implied in these changes. . Other names listed in a deed – especially in terms of small businesses, as it was the case here – are checked on a risk-sensitive basis which also takes into account whether the persons in question are personally known to the notary. The case was reported in the local news. Checks were carried out that concluded that no professional shortcomings occurred on the side of the notary profession. The case highlights how company registration can expose notaries to ML/TF risks and the need to ensure that customer due diligence is carried out in all instances, although the intensity of such checks should depend on the level of risk associated with the transaction/activity.

Case study - Italy[347]
A notary reported suspicious activities in relation to the creation of two limited liability companies, as well as the transfer of shares by a financial intermediary to one of the newly created companies. The notary suspected the companies to be linked to a strawmen, in light of inconsistencies between the declared beneficial owner and her economic profile, as well as of the presence of an unrelated person, already suspected of other similar activities, at the time of providing the notarial services. Checks confirmed analogies between the two companies, whose capital was decided upon and fully

[346] Luxembourg, 2020: *National Risk Assessment.*
[347] UIF (Italian Financial Intelligence Unit), July 2018: *Anti-money laundering booklets (ML/TF cases).*

subscribed on the same day, with full control exercised by the beneficial owner who however held no further share. The tax declarations of the beneficial owner dated back to the previous decade and were inconsistent with her role in the companies and relevant transactions. The beneficial owner declared to the notary that the capital had been subscribed through 8 cheques. However, the bank indicated by the beneficial owner could not confirm the origin of funds, nor that they had dealt with those funds, and that the beneficial owner was not their client. The report allows concluding that rules on the establishment and subscription of capital had not been respected. Further suspected illicit activities involved transactions with the financial intermediary.

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 groups 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 service provided by legal professionals has been considered together with money laundering vulnerabilities related to services from these professionals due to the increase take-up by terrorist groups of methods traditionally employed by organised crime groups. The terrorist financing threat therefore does not need a separate assessment.

Conclusion: The assessment of the terrorist financing vulnerability 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 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).

Innovation in the sector through the use of legal tech solutions has the potential of making the provision of services by the legal profession more effective and speedier. At the same time, document automation and off-the-counter solutions open up new vulnerabilities if standardisation is not accompanied by an adequate involvement of human intervention by the legal profession to assess money laundering and terrorist financing risks involved in the transaction/activity.

b) risk awareness

The sector is not homogeneously organised (scope of legal professionals varies from one Member State to another — although this isn't 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 order to improve understanding of AML/CFT requirements and ML/TF risks, a training package has been developed by the European Commission in cooperation with the EU Lawyers' Association (CCBE). 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 lawyers (although suspicious transaction reports from legal professionals cannot be compared to legal reports from financial institutions, for example). In the case of notaries, the situation is more varied and in some Member States the number of suspicious transaction reports by this profession constitutes a significant share of all reports submitted by professionals. This is however not the case across all Member States, and more the result of the specific approach by lawyers in certain Member States, which has led to a better understanding of risks, better detection of suspicions and increased reporting to the Financial Intelligence Units. Other solutions have also been adopted by Member States where the low reporting of suspicions was rather attributed to a wide interpretation of the legal privilege (see point c).

Self-regulatory bodies are generally active in providing general training on AML/CFT obligations.

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. As indicated in the sector description, fundamental differences also exist between lawyers and notaries in terms of their respective functions.

In any case, guaranteeing the protection of the anonymity of the legal professional reporting the suspicion remains a must. Risks 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 or appears on information leaked to the press expose these professionals disproportionally. To avoid this, rules exist that allow reporting of suspicions through the self-regulatory body.

The legal professional privilege (professional secrecy) is a recognised principle at EU level which reflects a delicate balance between the role of lawyers in the administration of justice and their role in the prevention of money laundering and terrorist financing (see in particular Case C-305/05 *Ordre des barreaux*). The principles underpinning the legal professional privilege are anchored in the judicial traditions of EU Member States, and are reflected in 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. Hence, the legal professional privilege cannot be invoked in all instances (see also ECHR Case *Michaud*, 2012).

Information collected by the Commission in the preparation of the AML Package of July 2021, European Semester work as well as through monitoring of implementation of EU law, combined with

findings of the EU Member States mutual evaluation reports by the Financial Action Task Force and Moneyval point to a generally low effectiveness of supervision regarding these professions. In particular, when supervision is performed by self-regulatory bodies data show that inspections are mainly focused on compliance with professional standards rather than with AML/CFT obligations, the risk-based approach is still nascent due to a lack of information on the level of risk of the supervised population and few to no supervisory measures are taken for breaches of AML/CFT obligations, if any breach is detected at all. Evidence from specific Member States' cases shows that this is in market contrast with a much higher detection of breaches for the same types of services detected by public supervisors.

Conclusions: The sector's awareness of the risks is not homogeneous, with a higher risk awareness on the side of notaries as opposed to lower measures applied by lawyers, as exemplified by the limited number of suspicions reported across all EU Member States despite the moderately to significantly high risk. 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 services provided by legal professionals is therefore considered as <u>significant</u> for lawyers (level 3) and moderately significant/significant for notaries.

Risk level

As regards **lawyers**, the level of threat has been assessed as significant (3), and the level of vulnerability has also been assessed as significant (3).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **notaries**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant / significant (2/3).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing/money laundering is HIGH for lawyers and MEDIUM/HIGH for notaries.

Mitigating measures

For the Commission:

- In the context of Directive (EU) 2015/849 as amended by Directive (EU) 2018/843:
  - Transposition and implementation checks on transparency requirements for beneficial ownership information: Member States should have in place strong regimes to ensure transparency of beneficial ownership information, based on a correct implementation of the definition of beneficial owner for corporate entities on the one hand and legal arrangements and foundations on the other.
  - To monitor the take-up of training activities by the legal profession on the basis of the training package completed.
  - In anticipation of the entry into force of the AML reform package, to continue dialogue on the implementation of the money laundering and terrorist financing requirement and to

raise awareness of and exchange best practices on different aspects of legal professionals' anti-money laundering compliance.

- In the context of transposition and implementation checks of Directive 2018/822/EU: Member States must report on measures to ensure that intermediaries submit information on reportable cross-border tax arrangements[348] to their national authorities.

For the competent authorities:

- Competent authorities/self-regulatory bodies should recall expectations that all elements of customer due diligence be performed in all cases, with the level of risk determining the intensity of the checks to be performed.
- 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 them immediately and unfiltered to the financial intelligence units. Self-regulatory bodies should draw up annual statistics on the number of reports filed to the financial intelligence units and assess their consistency with the risk exposure of the sector.
- On-site inspections should be carried out on a risk-sensitive basis following an AML/CFT risk assessment of their supervised population. To this end, supervisors should have a clear understanding of the services provided by the legal professionals and risks associated with them.

For Member States:

- Member States should provide guidance on typologies and risk factors arising from transactions involving independent legal professionals, lawyers, notaries.
- Member States / legal professions should assess the opportunities and challenges from the introduction of legal tech solutions.
- Member States should monitor the market to detect whether services that fall under the AML Directive are provided by entities that are not authorised legal professionals but who leverage legal tech solutions, and take the necessary mitigating measures.
- In line with the FATF standards, Member States should ensure that when supervision is performed by self-regulatory bodies, they are overseen, for AML/CFT purposes, by a public authority.
- Self-regulatory bodies should intensify inspections, whilst also strengthening the focus on AML/CFT aspects of their checks and ensure that supervision is risk-based.
- Training courses for lawyers should be organised on the basis of the material developed together with the European Commission to develop a better understanding of the risks and AML/CFT compliance obligations.
- Notaries associations should build on and replicate cases of peer reviews and mutual assistance in order to create synergies across borders and support a common understanding of the biggest risks facing the profession.

[348] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

GAMBLING SECTOR PRODUCTS

General description of the gambling sector

Under the current EU AML framework (the 4th AMLD as modified by the 5th AMLD, "the 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 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 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. By June 2021, 8 Member States notified exemptions to the European Commission, among which lotteries, Gaming machines outside casinos and bingo games are the most commonly exempted gambling services.

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, despite a conjectural drop in 2020 and 2021 due to the COVID-19 crisis. Europe's total gambling

revenue is estimated EUR 75.9 billion in 2020, (23% drop compared to EUR 98.6 billion gross gaming revenue in 2019)[349]. Online gambling revenues in the EU and the UK were estimated at around EUR 26.3 billion in 2020, against 16.5 billion in 2015. The revenue of the offline/land-based gambling market has also declined from around EUR77.5 billion in 2015 to around EUR 49.6 billion in 2020, due to the shuttering of land-based establishments during the COVID 19 crisis. A noticeable trend expected to continue is the increasing popularity of the use of mobile devices for online betting, with mobile betting expected to account for 45.6% of Europe's online gambling revenue in 2020 and to reach 50.8% by 2022, surpassing the use of desktop for the first time. This trend is expected to continue, with mobile betting projected to reach a 58.2% share in 2025.

Through non-legislative actions, as set out in the 2012 Communication 'Towards a comprehensive European framework for online gambling'[350], 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[351], 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.

[349] Data from the European Gaming and Betting Association (EGBA): https://www.egba.eu/news-post/europes-gambling-revenues-to-drop-23-in-2020-but-online-maintains-growth-new-data/
[350] COM(2012) 596 final.
[351] Commission Recommendation of 14 July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online (Text with EEA relevance), *OJ L 214 19.07.2014, p. 38.*

1. 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)[352];

(3) a perpetrator places money in a betting account in one location and an accomplice withdraws the funds in another (concealment, disguise and transfer)[353].

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

[352] Note that if the withdrawal is in cash and there is no winning 'certificate' issued by the casino/betting platform, this cannot qualify as money laundering.
[353] This scenario should be only possible in online betting or in a non-compliance land-based service.

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.
- The combination of betting with cryptocurrencies should as well be highlighted. Indeed, some platforms are allowing betting with cryptocurrencies as a payment method. Additionally, standards of due diligence followed by those platforms are not necessarily optimum.

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[354];
- customers regularly requesting receipts when collecting machine winnings[355].

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"[356] 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. With the exception of casinos, Member States may additionally decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing the 4th AMLD, following an appropriate risk assessment and on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

[354] The rule should be that the mean of payment to receive winnings is the same than the one that was used for the initial payment. If there are large winnings, the customer could request for winnings in another payment method/mean but after thorough checks that the winnings are actually winnings. Another very important point is that when the customer cashes out his account, and if he used a credit card or a bank account, the "cash out" should be deposited in the same card or account. However, these rules are not harmonized across the EU.
[355] This is not a problem in itself as long as the betting service is checking the winnings and is carrying out proper due diligence.
[356] "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.

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).

Conclusions: 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 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).

Risk level

As regards terrorist financing, the level of threat and the level of vulnerability have been assessed as **not relevant.**

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as significant (3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
➔ 2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusion: estimated risk level for money laundering is level 3, HIGH. The question of the risk level for terrorism financing is deemed not relevant.

Mitigating measures

For the 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:
    - o strengthening the detection of suspicious transactions and increasing the number and the quality of the suspicious transaction reports;
    - o 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;
    - o 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;
    - o 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;
    - o developing standardised template(s) at EU level for suspicious transaction or suspicious activity reports taking into account specific characteristics of the gambling sector.
- Member States shall, before granting possible exemptions of AML/CFT requirements to specific gambling services, carry out a risk assessment with a focus on:
    - money laundering and terrorist financing vulnerabilities and mitigating factors of the exempted gambling services;
    - the risks linked to the size of the transactions and payment methods used;
    - the geographical area in which the exempted gambling service is administered.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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

    - players' cards[357] or the use of electronic identification schemes in order to facilitate customer identification and to limit the use of cash, and
    - 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 EUR 2,000 as provided by Article 11 d) of Directive (EU) 2015/849, whether the transaction is carried out in a single operation or in linked transactions).
- Consider the introduction of harmonized rules on the payment methods.
- Ensure strict due diligence when payment method is crypto

For the Commission:

- In the last (2019) SNRA, it was proposed that 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'. The new Commission "Proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" provides a definition of a linked transaction, which means "two or more transactions with either identical or similar origin and destination, over a specific period of time".

[357] "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.

2. 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. With the exception of casinos, Member States may additionally decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing the 4th AMLD, following an appropriate risk assessment and on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services. By June 2021, 8 Member States had notify such exemptions, including for 5 of them exemptions related to bingo.

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.

Conclusions: 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).

Risk level

As regards terrorist financing, the level of threat and the level of vulnerability have been assessed as **not relevant.**

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as low (1), while the level of vulnerability has been assessed as low (1).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusion: estimated risk level for money laundering is level 1, Low. It is deemed not relevant for terrorism financing.

Mitigating measures

For the competent authorities:

- 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.
- Before granting possible exemptions of AML/CFT requirements to specific gambling services, Member States shall carry out a risk assessment with a focus on:
  - money laundering and terrorist financing vulnerabilities and mitigating factors of the exempted gambling services;
  - the risks linked to the size of the transactions and payment methods used;
  - the geographical area in which the exempted gambling service is administered.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

3. 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 or land-based) 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 and Ireland) 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)[358].

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[359].

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[360].

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[361].

[358] If the initial payment is in cash and cash is received back and if there is no winning ticket then it cannot qualify as ML.
[359] As previous comment. Also, casinos should check if such customer really won before giving a winning ticket. EU casinos usually do and do not provide winning tickets.
[360] Albeit this would be in principle more a fraud against the casino than a ML scheme.
[361] This shouldn't happen in an EU casino under normal circumstances. A customer could have an account in one casino (and within a branch of that casino), but another customer could not cash out from the same account as it is owned by another person.

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 could 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.

Conclusions: Casinos are considered to be exposed to infiltration risks, although for casinos owned by the State or public companies, this level of risk is lower. 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 moderately significant (level 2).

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. Crypto-ATMs installed in land-based casinos can be considered as a risk. Customers can withdraw cash directly from those ATMs to bet and thereby laundering criminal crypto-assets.

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 moderately significant (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)

Risk level

As regards terrorist financing, the levels of threat and vulnerability have been assessed as **not relevant.**

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderately significant (level 2), while the level of vulnerability has been assessed as moderately significant (level 2).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusion: estimated risk level is deemed not relevant for terrorism financing. Estimated risk level for money laundering is level 2, MEDIUM.

Mitigating measures

For the 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:
    - o strengthening the detection of suspicious transactions and increasing the number and the quality of the suspicious transaction reports;
    - o 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;
    - o 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.
    - o 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;
    - o developing standardised template(s) at EU level for suspicious transaction or suspicious activity reports, taking into account specific characteristics of the gambling sector;
    - o 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.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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
    - players' cards[362] or use electronic identification schemes in order to facilitate customer identification and to limit the use of cash and
    - 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 are aware of the higher risk of money laundering when crypto-ATMs are installed in land-based casinos.
- 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 EUR 2,000 as provided by Article 11 d) of Directive (EU) 2015/849).

For the Commission:

- 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'.
- 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 EUR 2,000 as provided by Article 11 d) of Directive (EU) 2015/849, whether the transaction is carried out in a single operation or in linked transactions).
- In the last (2019) SNRA, it was proposed that 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'. The new Commission "Proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" provides a definition of a linked transaction, which means "two or more transactions with either identical or similar origin and destination, over a specific period of time".

[362]"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.

4. 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[363] 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.

[363] "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.

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 moderately significant (level 2).

Vulnerability

Terrorist financing

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. With the exception of casinos, Member States may decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing the 4th AMLD, following an appropriate risk assessment and on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services. By June 2021, 8 Member States had notify such exemptions, including for 4 of them exemptions related to gaming machines.

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 EUR 100 000 for failing to prevent a drug dealer from laundering over EUR 1 million in its outlets). However, gaming machines operators are currently developing some mitigating measures, 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).

Risk level

As regards terrorist financing, the level of threat and the level of vulnerability have been assessed as **not relevant.**

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderate (2), while the level of vulnerability has been assessed as moderate (2).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for money laundering is level 2, Moderate. It is deemed not relevant for terrorism financing.

Mitigating measures

For the 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:
    - o strengthening the detection of suspicious transactions and increasing the number and the quality of the suspicious transaction reports;
    - o 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;
    - o 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;
    - o ensuring supervisory authorities provide clearer guidance on emerging risks linked to video lottery terminals;
    - o 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;
    - o developing standardised template(s) at EU level for suspicious transaction or suspicious activity reports, taking into account specific characteristics of the gambling sector.
- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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
    - players' cards[364] or the use of electronic identification schemes in order to facilitate customer identification and to limit the use of cash, and
    - real-time monitoring systems to identify suspicious transactions at point of sale.
- 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 EUR 2,000 as provided by Article 11 d) of Directive (EU) 2015/849, whether the transaction is carried out in a single operation or in linked transactions).
- Before granting possible exemptions of AML/CFT requirements to specific gambling services, Member States shall carry out a risk assessment with a focus on:
    - money laundering and terrorist financing vulnerabilities and mitigating factors of the exempted gambling services;
    - the risks linked to the size of the transactions and payment methods used;
    - the geographical area in which the exempted gambling service is administered.

For the Commission:

- In the last (2019) SNRA, it was proposed that 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'. The new Commission "Proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist

[364] "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.

financing" provides a definition of a linked transaction, which means "two or more transactions with either identical or similar origin and destination, over a specific period of time".

5. Lotteries

Product

Lotteries

Sector

Gambling sector

General description of the sector and related product/activity concerned

Lotteries cover a wide range of numeric games where a winner is selected by chance. Lotteries range from national lotteries 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. EUR 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. 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[365].

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

[365] Here the most usual risk is when a criminal buys with illicit funds (cash) a winner lottery from another person who actually won.

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).

Risk level

As regards terrorist financing, the level of threat and the level of vulnerability have been assessed as **not relevant.**

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderate (2), while the level of vulnerability has been assessed as moderate (2).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for money laundering is level 2, Moderate. The question of the risk level for terrorism financing is deemed not relevant.

Mitigating measures

For the 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:

o 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;
o 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;
o 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;
o 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;
o developing standardised template(s) at EU level for suspicious transaction and suspicious activity reports, taking into account specific characteristics of the gambling sector.

- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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
    - the use of systems for systematically identifying winners, such as players' cards[366] or electronic identification schemes, in order to facilitate customer identification, and
    - the use of account-based fund transfers for payments of large amounts.
- Member States should encourage lotteries to designate an AML officer at the premises, 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 EUR 2,000 as provided by Article 11 d) of Directive (EU) 2015/849, whether the transaction is carried out in a single operation or in linked transactions).

For the Commission:

In the last (2019) SNRA, it was proposed that 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'. The new Commission "Proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" provides a definition of a linked transaction, which means "two or more transactions with either identical or similar origin and destination, over a specific period of time".

[366] "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.

6. Poker

Product

Poker (land-based/offline)

Sector

Gambling sector

General description of the sector 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. 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[367].

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

[367] If cash is here only changing hands, there is no ML. ML might occur if the winner received a winning ticket for this. The winning ticket is key.

- 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 significant (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. With the exception of casinos, Member States may additionally decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing the 4th AMLD, following an appropriate risk assessment and on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services. By June 2021, 8 Member States had notify such exemptions, but none for poker.

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).

Risk level

As regards terrorist financing, the level of threat and the level of vulnerability have been assessed as **not relevant.**

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as moderate (3), while the level of vulnerability has been assessed as moderate (3).

➔

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusion: estimated risk level for money laundering is level 3, High.

Mitigating measures

For the 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:
    - o strengthening customer due diligence requirements and the detection of suspicious transactions, and increasing the number and the quality of the suspicious transaction reports;
    - o 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;
    - o 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;
    - o 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;
    - o developing standardised template(s) at EU level for suspicious transaction and suspicious activity reports taking into account specific characteristics of the gambling sector.

- Before granting possible exemptions of AML/CFT requirements to specific gambling services, Member States shall carry out a risk assessment with a focus on:
    - money laundering and terrorist financing vulnerabilities and mitigating factors of the exempted gambling services;
    - the risks linked to the size of the transactions and payment methods used;
    - the geographical area in which the exempted gambling service is administered.

- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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 EUR 2,000 as provided by Article 11 d) of Directive (EU) 2015/849, whether the transaction is carried out in a single operation or in linked transactions).

For the Commission:

In the last (2019) SNRA, it was proposed that 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'. The new Commission "Proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" provides a definition of a linked transaction, which means "two or more transactions with either identical or similar origin and destination, over a specific period of time".

7. 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'[368] 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.

[368] 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.

It is to be noted that the EU is about to further align its AML/CTF legislation with the FATF standards on virtual assets. In that context, the Commission should review the current AML/CTF framework and assess the possibilities to better tackle the challenges posed by in-game currencies and gaming platforms that operate as **virtual asset service provider.**

Threat

Terrorist financing

The assessment of the terrorist financing threat related to online gambling has not been considered as relevant in the last supranational risk assessment report. However, terrorists could, increasingly use tokens qualifying as crypto-assets to sustain their activities. So far there are a few instances of Islamic and right-wing terrorist groups using virtual currencies for financing (e.g. bitcoin fundraising by Hamas in 2019[369], which is a case more relevant for the crowd funding analysis). On the other hand, there is no evidence that terrorist groups have used online gaming platforms to finance themselves and it seems that more conventional forms of financing (e.g. cash) are still predominating. Overall, the insufficiently regulated gaming economies offer a potential for future abuse by terrorists, who would be able to transfer and withdraw money almost untraceably.

Conclusions: with the exception of in-game currencies (that cannot be exchanged), the exchangeable tokens used in video game can be assimilated to crypto-assets. Therefore, their threat assessment should follow the same regime. In that context, the level of the threat posed by online gambling for terrorism financing is considered as very significant (level 4).

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.
- 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.

[369] During an online fundraising campaign led in January 2019, the armed wing of Hamas asked to its supporters to make donations through the digital currency Bitcoin thanks to a two-minute video on the al-Qassam Brigades website showing step-by-step instructions in Arabic allowing to avoid the traditional financial system and donate cryptocurrency. https://www.reuters.com/article/us-crypto-currencies-hamas/hamas-shifts-tactics-in-bitcoin-fundraising-highlighting-crypto-risks-research-idUSKCN1S20FA

- 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 very significant (level 4).

Vulnerability

Since they enable the trade of *de facto* convertible in-game currency, online gaming platforms, in general, should be considered and thus regulated like crypto-asset service providers[370] (CASPs).

Terrorist financing

a) risk exposure

When used anonymously, gaming tokens qualifying as crypto-assets could be used 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 crypto-assets 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 crypto-assets 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 but competent authorities and financial intelligence units have noted in their contacts with the on-line gambling services providers sector that the level of awareness of terrorist financing risk is still rather low.

[370] According to the FATF, a "*Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset*".

The most important emerging risks are 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 gaming platforms but also financial and credit institutions to increased risks of money laundering and terrorist financing where they act as intermediaries or exchange platforms between tokens qualifying as crypto-assets 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 introduced a first EU definition of crypto-assets 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. While related provisions should have been transposed by all Member States in January 2020, it is not fully the case yet[371].

The European Commission's proposal for a Regulation on Markets in Crypto-assets[372] (MiCA) published in September 2020 will have, if adopted, the effect of expanding the EU regulatory perimeter to a wide range of crypto-asset activities. Further action is expected in 2021 with the publication of the EU's proposals to strengthen the EU's AML/CFT framework, including a proposal to align the scope of the AMLD with the activities covered by MiCA.

Conclusions: with the exception of in-game currencies (that cannot be exchanged), the exchangeable tokens used in video game can be assimilated to crypto-assets. Therefore, their threat assessment should follow the same regime. In that context, the level of the threat posed by online gambling for money laundering is considered as very significant (level 4).

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).

[371] Anti-money laundering directive - transposition status (last updated in April 2022).
[372] Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - COM/2020/593 final.

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[373] 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.

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. With the exception of casinos, Member States may additionally decide to exempt, in full or in part, providers of certain gambling services from national provisions transposing the 4th

[373] An entity that provides services to safeguard private cryptographic keys on behalf of their customers, to hold, store and transfer virtual currencies.

AMLD, following an appropriate risk assessment and on the basis of the proven low risk posed by the nature and, where appropriate, the scale of operations of such services.

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 EU online operators[374] (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 very significant (level 4).

[374] Online operators within EU jurisdictions only. There are many operators located in third countries, offering service to EU nationals and facilitating money laundering who do not apply the same risk-based measures. For EU law enforcement and judicial authorities, it is very difficult to receive information (even with judicial warrants) from operators located outside of the EU or from operators located in the EU but who have servers located outside of the EU.

Risk level

As regards terrorist financing, the level of threat has been assessed as very high (4), while the level of vulnerability has been assessed as very high (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as very high (4), while the level of vulnerability has been assessed as very high (4).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
➔ 3,6 – 4	Very significant VERY HIGH

Conclusion: estimated risk level for online gambling is level 4, VERY HIGH, for both money laundering and terrorism financing.

Mitigating measures

For the 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 online gambling and provide efficient guidance.
- Member States should ensure regular cooperation between relevant authorities and online gambling operators, which should focus on:
    - o 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;
    - o 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;
    - o 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;
    - o 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;
    - o 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.
- Before granting possible exemptions of AML/CFT requirements to specific on-line gambling services, Member States shall carry out a risk assessment with a focus on:
    - money laundering and terrorist financing vulnerabilities and mitigating factors of the exempted on-line gambling services;
    - the risks linked to the size of the transactions and payment methods used;
    - the geographical area in which the exempted on-line gambling service is administered.

- Considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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, whether the transaction is carried out in a single operation or in linked transactions).
- 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.

For the Commission:

- In the last (2019) SNRA, it was proposed that 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'. The new Commission "proposal for a regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing" provides a definition of a linked transaction, which means "two or more transactions with either identical or similar origin and destination, over a specific period of time".
- Online gambling service providers operating within EU should have a legal presence within the EU in order to attend all judicial requests and to apply EU legislation.

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

At present, there is neither a common legal definition of a non-profit organisation in EU law, nor a comprehensive legislative framework at EU level in that field. Thus, NPOs are not directly included in the EU AML/CFT framework, following a similar approach as for other legal entities, foundations and legal arrangements in Union law and under the international standards of the Financial Action Task Force (FATF). However, at international level, the FATF has adopted a functional definition of an NPO in its **Interpretive Note to Recommendation 8** as '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"[375]. This definition is also used by the European Commission for the purposes of this risk assessment.

NPOs in the European Union are very heterogeneous in size and legal form[376]. Rules for registering a NPO, supervision and reporting obligations vary between Member States. In addition, NPOs play an important role as facilitators of broad policy dialogue, which is closely linked to the fundamental rights of citizens to form associations in order to pursue a common purpose in modern democracies. Their critical role has been highlighted in various reports (e.g. in a UN Counter-terrorism Implementation Task Force Working Group Report[377]).

For the purpose of this risk assessment, a distinction is made between ***expressive*** and ***service NPOs.*** While expressive NPOs are predominantly involved in expressive activities (e.g. programmes focused on sports and recreation, arts and culture, interest representation, and advocacy), service NPOs are involved in diverse activities (e.g. programmes focused on providing housing, social services, education, or health care).

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[378]). Humanitarian NPOs may be active in and outside Europe, and in different operational contexts.

---

[375] http://www.fatf-gafi.org/publications/fatfgeneral/documents/plenary-outcomes-june-2016.html#npo

[376] Commission Communication "Promoting the role of voluntary organisations and foundations in Europe" COM(1997)241 https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0620:FIN:EN:PDF

[377] UN Counter-terrorism Implementation Task Force (CTITF) Working Group Report on "Tackling the Financing of Terrorism" of October 2009 available at: https://www.un.org/counterterrorism/ctitf/sites/www.un.org.counterterrorism.ctitf/files/ctitf_financing_eng_final.pdf

[378] The principles' centrality to the work of humanitarian organizations is formally enshrined in two General Assembly resolutions. The first three principles (humanity, neutrality and impartiality) are endorsed in General Assembly resolution

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. The humanitarian aid sector covers a wide range of organisations with varying degrees of operational and organisational capacity. A large segment of NPOs receives humanitarian aid funding, including from the EU and from Member States. These are subject to a strict contractual framework with a high degree of safeguards[379].

Description of the risk scenario

Assessing the whole NPO sector is challenging due to the sector's overall diversity and because each NPO sub-sector faces a different level of risk/threat[380]. In addition, the analysis showed that the NPO sector might be subject to de-risking by financial institutions, which limits their functioning through financial exclusion and increases the risks[381].

Expressive and service NPOs face a different level of risk due to their nature of activity. While expressive NPOs may be infiltrated by criminal or terrorist organisations that can hide the beneficial ownership and making the traceability of financial flows more difficult, service NPOs may be more directly vulnerable due to the intrinsic nature of their activity that involves funding to and from conflict areas or third countries identified by the Commission as presenting strategic deficiencies in their anti-money laundering and countering the financing of terrorism regimes[382].

The risk scenario covers the establishment of an NPO under the pretext of collecting donations for charitable activities and collection of funds by an NPO and transfers of funds from it to project partners/beneficiaries. It also covers the internal infiltration of the NPO. 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. It also reflects the threat stemming from the flow of funds from third countries to the internal market (especially the undesirable foreign influencing of national civil and religious organisations through non-transparent financing, which has been highlighted by the European Council conclusions of 11 December 2020[383].

When dealing with the risks at hand, a fundamental distinction must be made between ***intentional complicity*** and those NPOs that have been ***exploited unknowingly,*** as these situations require different

46/182, which was adopted in 1991. General Assembly resolution 58/114 (2004) added independence as a fourth key principle underlying humanitarian action.
https://www.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf

[379] 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) or, since 2021, a 'Certificate'. 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.

[380] 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.

[381] According to EBA (Opinion of the European Banking Authority on 'de-risking', EBA/Op/2022/01), de-risking can be a legitimate risk management tool, but it can also be a sign of ineffective ML/TF risk management, with possible severe consequences. EBA considers that its regulatory guidance on how to manage ML/TF risks, if applied correctly, should help avert unwarranted de-risking:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf

[382] Commission Delegated Regulation (EU) 2022/229 of 7 January 2022 on amending Delegation Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council.

[383] https://www.consilium.europa.eu/media/47296/1011-12-20-euco-conclusions-en.pdf

responses. While cases of complicit NPOs require enhanced oversight and financial control, cases of exploited NPOs call for information sharing with authorities about partners and beneficiaries. Although transparency is important for any organization, in the case of NPOs, it is especially relevant to demonstrate that the resources they receive are used to fulfil the purpose for which these organizations were conceived[384].

To reach the necessary granularity when dealing with such a complex reality like NPOs and to determine the risks levels affecting the sector special consideration has been given to the information provided by, mainly, the National Risk Assessments (NRA) prepared by the Member States. Some of them (Denmark, for instance) have prepared individual, detailed assessments for the sector, while most of them treat NPOs under thorough assessments as a dedicated chapter within their NRA (e.g.: Finland, Spain, Italy, Germany).

Threat

Terrorist financing

NPOs may be infiltrated by terrorist groups[385], which may then represent a significant threat, in particular as concerns the funding of foreign terrorist fighters, though there is no comprehensive information how common this method is being used by terrorist groups across Member States. In general, the collection and transfer of funds through NPOs is regulated by various national, and sometimes regional, laws. In line with the FATF recommendations to apply focused and proportionate measures to NPOs to protect them from TF misuse, almost all Member States have some kind of supervision over NPOs, either through tax authorities, charity regulators or other types of supervising authorities. 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, depending on the funding sources (unknown/cash/international sources/high-risk countries), how funds are being distributed, the types of activity, or beneficiaries (unknown/high-risk countries/high-risk customers/use of informal channels for sending money across borders). These risks increase when no formal banking channels are available for money transfers to and by NPOs due to de-risking practices by financial institutions. New technological tools such as crowdfunding and block chain systems might also be misused by or through

[384] Cristina Ortega-Rodríguez, Ana Licerán-Gutiérrez and Antonio Luis Moreno-Albarracín: "Transparency as a Key Element in Accountability in Non-Profit Organizations: A Systematic Literature Review"; *Sustainability* 2020, 12, 5834; doi:10.3390/su12145834, https://www.mdpi.com/journal/sustainability

[385] This is not a theoretical risk and has been treated at length, among others, in the following official reports:

- FATF Report, "Risk of terrorist abuse in non-profit organisations", 2014: https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf
- NPO/NGO sector assessment of Bangladesh: https://www.bb.org.bd/pub/research/sp_research_work/srw1505.pdf (The report expressly estates *"Terrorist organisations have taken advantage of these characteristics of NPOs to infiltrate the sector and misuse NPO funds and operations to cover for, or support, terrorist activity"*.)
- This risk was also raised by the United Nations Office on Drugs and Crime (UNODC) back in 2012: "The use of the Internet for terrorist purposes", https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
- The Council of Europe also raised this issue, specifically as regards Serbia, in its "The risks to non-profit organisations of abuse for money laundering and terrorist financing in Serbia", 2013: https://rm.coe.int/the-risks-to-non-profit-organisations-of-abuse-of-mlterrorist-financin/16807828e5
- AUSTRAC — the Australian Transaction Reports & Analysis Centre — considers that Non-profit organisations (NPOs) operating in Australia and throughout South-East Asia are vulnerable to terrorist infiltration and exploitation, and concluded that links had already been identified between terrorist groups and NPOs in Australia (2018): https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf

NPOs, 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.

The work of humanitarian NPOs may take place in areas which are at times high risk[386] 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 professionalization of an NPO and the situation in that particular country, including the political dynamics of the conflict in question.

Cases for study – A case for risk-based approach[387]

In the past some terrorist groups have exploited or used charities as a front for building support. This has been the case, for instance, for Irish republican terrorists, Sri Lankan separatists, Lebanese extremists, Kashmiri terrorists…

In today's world, similar organisations are already included in wide-effect lists of terrorist groups. This, as well as the introduction of international standards have made their involvement in similar operations much more complicated.

Nevertheless, international standards have also been seen as making it harder for NPOs to intervene neutrally amidst conflict and limited civil society activities more generally. The fact is that while some terrorist organisations seek to exploit charitable connections, **very few charities have been actually tied to money laundering or the financing of terrorism**. In conclusion a **risk-based approach** is necessary.

Syria aid convoy

In 2013, two British citizens joined a massive British aid convoy and set off to hand cash – intended to buy weapons – over to terrorist fighters in Syria. The humanitarian mission involved 100 vehicles including ambulances and large lorries packed with supplies. **There was no suggestion in the trial that the convoy's organisers knew of the pair's plans.**

This was the first court verdict in the United Kingdom showing that some aid convoys were abused. The outcome of the case raised questions about whether charities organising humanitarian convoys, to transport aid and medical supplies to foreign conflict zones, have the means to identify potential abuse - and whether they are capable of stopping it.

The Europol TE-SAT 2022[388] provides some examples that could be considered as case studies or examples of TF:

(a) There are instances of terrorist groups using non-profit organisations to collect donations under the guise of charitable collections. In Spain, three suspects were arrested for terrorism financing by using these means. The money was raised by a religious organisation under the pretence of humanitarian aid for Syrian orphans, but it was diverted to fund al-Qaeda fighters in Syria by using a non-profit organisation. Some foundations openly collect funds for FTFs and their families in conflict zones and prison camps in Syria. In addition, family and friends also financially contribute to jihadists outside of the EU (page 17).

(b) Other ways of generating income include the online sale of merchandise on e-commerce platforms (band t-shirts, CDs and World War II Nazi equipment in a right-wing context),

[386] E.g. civil unrest, lack of state control, military conflict zones, …

[387] A good introduction: Ly, Pierre-Emmanuel, "The charitable activities of terrorist organizations", *Public Choice*, Vol. 131, No. 1/2 (Apr., 2007), pp. 177-195: https://www.jstor.org/stable/27698091

[388] https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

membership fees, and publications and tickets for events organised by affiliated NGOs for ethno-nationalist and separatist groups. (page 18).

(c) Several Western Balkan countries confirmed the trend seen in previous years whereby some extremist groups portray themselves as non-governmental organisations (NGOs) working for humanitarian aims. In this position, they collect donations which are then channelled to supporters or sympathisers of radical Islamist ideologies. In some cases, these groups established links with migrant communities originating from the Western Balkans in EU countries (page 37).

Conclusions: For NPOs collecting or transferring funds the estimated 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 estimated level of threat of TF 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. Nevertheless, this assessment also considers that, while the threat certainly exists, the scarce number of actual cases of NPOs having been misused for money laundering needs to be considered within a balanced conclusion.

Conclusions: For NPOs collecting or transferring funds the estimated level of threat 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 estimated level of threat for ML 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

Due to the diversity of the sector, a risk analysis from a vulnerability perspective of the NPO sector as a whole is difficult.

a) risk exposure

As mentioned above, some NPOs may be exposed to risks. Small amounts of funding are in cash (virtual assets, in a handful of cases), which makes it difficult for law enforcement agencies and financial intelligence units to trace the sources of funds and transfers sent abroad. In line with the threat assessment, the risk exposure also increases through financial exclusion of NPOs, especially banking de-risking (possibly declining correspondent banking).

The work of humanitarian NPOs may take place in areas which are at times high risk[389] and where non-state armed groups or persons designated as terrorists are present. The specific risks depend on various

[389] E.g. civil unrest, lack of state control, military conflict zones, …

factors, however, such as the level of professionalization 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, though mostly indirectly through financial institutions during the course of customer due diligence obligations (e.g. when a NPO is subject to CDD practices or confronted with de-risking practices). Some NPOs already undertake their own risk assessments, taking into account the location, type of activity, and the organisation's past involvement in the area and relationships with other sectors. They continue to develop a and refine controls and due diligence measures for the transfer and collection of funds (sanction lists, transaction screening). There are some developments where the sector is also developing and participating in peer-learning exchanges on due diligence practices, transparency and accountability issues and risk management, as well as awareness-raising on terrorist financing.

In some Member States there is greater collaboration and outreach to the banking sector to facilitate safe and regulated channels for legitimate humanitarian causes, which boosts transparency and helps safeguard NPOs from misuse and influencing by terrorists, while at the same time allowing humanitarian aid to be delivered to those regions most in need. However, it is unclear if these practices are applied across all Member States and in collaboration with the whole NPO sector.

There is currently no clear overview of the sector's engagement in self-regulation, the development of codes of conduct.

It appears that especially larger and well established 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 in relation to donor requirements and to ensure that the aid reaches its intended beneficiaries. In addition, NPOs receiving humanitarian aid funding from the EU and from Member States are subject to a strict contractual framework with a number of safeguards.

While the NPO sector is vitally important for providing humanitarian assistance around the world, it is difficult to assess the sector's overall risk awareness because of the sector's diversity and the changing circumstances it is operating in. To safeguard the legitimate objectives of such assistance, more information about terrorist financing risks within the NPO may be needed 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[390]. 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 headquarters and

[390] This is exemplified especially in the NRA provided to the Commission by the Member States.

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 agreement[391].

The 2005 Commission Communication on the prevention of and fight against terrorist financing through enhanced national level coordination and greater transparency of the non-profit sector[392] introduced a recommendation to Member States to address the vulnerabilities of the non-profit sector to terrorist financing and other criminal abuse while also enhancing donor confidence and encouraging donations. Following the recommendation, Member States should ensure that they have oversight over their NPO sector and ensure national cooperation if a public body or bodies are entrusted with the oversight of the NPO sector or part of it. It was further recommended that Member States should encourage compliance with the proposed Code of Conduct, which was included in this Communication. The recommendation also highlighted the importance that both Member States and their NPOs are fully aware of how organisations may be misused for terrorist financing and other criminal purposes and the need for proportionate investigations of abuse of NPOs by following existing criminal law procedures.

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 counterterrorism agenda and the legitimate objectives of humanitarian NPOs[393].

Conclusions: For NPOs collecting or transferring funds the estimated 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 estimated level of TF vulnerability 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: For NPOs collecting or transferring funds the estimated 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 estimated level of vulnerability for ML is considered as less significant (level 1).

[391] A 'Framework Partnership Agreement' until end of 2020. Since 2021, a 'Certificate'.

[392] Commission Communication to the Council, the European Parliament and the European Economic and Social Committee on "The Prevention of and Fight against Terrorist Financing through enhanced national level coordination and greater transparency of the non-profit sector", COM(2005) 620 final of 29 November 2005.

[393] For example, Recital 38 of 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 excludes the provision of humanitarian activities by impartial humanitarian organisations from its scope.
Also, UNSCR 2642 (2019) refers to terrorism financing while not mentioning NPOs specifically. Similarly, the Council Conclusions on EU External Action on Preventing and Countering Terrorism and Violent Extremism of 16 June 2020.
Last but not least, the Council conclusions of 11 December 2020 mention the "foreign influencing of national civil and religious organisations through non-transparent financing".

Risk Level

As regards **terrorist financing**, the estimated level of threat for NPOs collecting or transferring funds has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant (2).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

As regards **money laundering**, the estimated level of threat for NPOs collecting or transferring funds has been assessed as moderately significant (2), while the level of vulnerability has been assessed as moderately significant (2).

RISK	
1 – 1,5	Lowly significant LOW
➔ 1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: the estimated risk levels for terrorist financing and money laundering for NPOs collecting or transferring funds is MEDIUM

For NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, as regards **terrorist financing,** the level of threat has been assessed as less significant (1) and the level of vulnerability has been assessed as less significant (1).

RISK	
➔ 1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

For NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, as regards **money laundering**, the level of threat has been assessed as less significant (1) and the level of vulnerability has been assessed as less significant (1).

RISK	
➔ 1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

Conclusions: the estimated risk level for NPOs receiving institutional funding, among others by the EU or Member States in charge of the management of EU funds, for terrorist financing and money laundering is LOW.

Mitigating measures

FATF recommends the adoption of measures that *"do not disrupt or discourage legitimate charitable activities, and should not unduly or inadvertently restrict NPOs' ability to access resources."*

In February 2021, the Financial Action Task Force (FATF) launched a new project to study and mitigate the unintended consequences resulting from the incorrect implementation of the FATF Standards, including de-risking, financial exclusion and undue targeting of NPOs[394].

[394] https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/unintended-consequences-project.html

For the Commission:

- The Commission should consider analysing the steps taken – if any – by Member States in order to understand the risks and vulnerabilities of the sector and their measures to protect the sector from abuse of ML/TF, as well as the steps taken – if any – by the NPO sector to promote transparency and accountability, raise awareness of the risks and vulnerabilities of the sector, including the development of best practices to mitigate the risks.
- The Commission should also analyse and try to better understand what types of categories of NPOs are more susceptible to TF threat and risks and what features/qualities make certain NPOs more susceptible to risks – to again continue with developing a more nuanced approach to this sector.
- Continue to engage with NPOs that receive EU funding on the relevant EU AML/CTF 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 promoting the introduction of a risk-based approach involves pinpointing where threats can exploit vulnerabilities.

For the Member States:

- Member States should ensure that they are fully aware of the risks and vulnerabilities of the sector and that their measures to protect the sector from abuse for money laundering or terrorist financing are focused and proportionate.
- Member States should ensure that their NPO sector is fully aware of how organisations may be misused for money laundering or terrorist financing and how to mitigate these risks.
- 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.
- Member States should support NPOs by providing awareness-raising materials for NPOs (at Member State level as well as EU level).
- Member States should ensure that they apply focused and proportionate measures to NPOs in order to protect them from possible ML/TF abuse.
- Member States should ensure that the sector is not subject to de-risking by financial institutions, leading to their financial exclusion.
- Member States should ensure that they have oversight over their NPO sector and ensure national cooperation if a public body or bodies are entrusted with the oversight of the NPO sector or part of it.
- Member States should encourage compliance with the Code of Conduct proposed with the 2005 Commission Communication on the prevention of and fight against terrorist financing through enhanced national level coordination and greater transparency of the non-profit sector[395].

[395] Commission Communication to the Council, the European Parliament and the European Economic and Social Committee on "The Prevention of and Fight against Terrorist Financing through enhanced national level coordination and greater transparency of the non-profit sector", COM(2005) 620 final of 29 November 2005.

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[396].

Like many other businesses, sport and gambling have been consistently used by criminals to launder money and derive illegal income. As in the art world, criminals in the sports world are not always only 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.

According to EUROPOL, the involvement of organised crime groups in sports corruption, and in particular in match-fixing, often exploiting the sports sector for sports corruption and money laundering purposes at the same time. The most affected sports are football and tennis, however intelligence suggests that other professional sports are also targeted by organised crime groups (e.g. basketball, handball, beach volleyball, horse racing, ice hockey).

The global betting market across all sports is estimated to be worth $1.7 trillion per year. Against this scenario, betting-related match fixing can serve as a platform to further high-scale money laundering schemes by the same organised crime groups involved in sports corruption for its own benefit and/or serve other organised crime groups in search of specialised 'laundering services.' Money laundering takes place via online betting, either by exploiting regulated betting operators or by taking direct ownership of these operators.

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

[396] As an overview for the whole general description: EUROPOL, "The involvement of organised crime groups in sports corruption", 5.08.2020. See also the FATF report "Money laundering through the football sector", July 2009.

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.

The development of national and international player transfer markets, linked to a continuous increase in the valuation of professional players offers more and more opportunities for criminals to defraud or launder money.

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 with the assistance of confederations. It has the authority to promote and develop football globally. Each country has a national association 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)[397], 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 cooperates with 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.

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 statutes were approved at the70th FIFA Congress, on 18 September 2020, and became effective on the same day. Changes to the FIFA statutes can only be made by a Congressional session and require a 75% majority of national federations present

[397] From 13 July 2020FIFA's new Code of Ethics (CoE) has come into force.

and entitled to vote. This makes FIFA statutes and their implementing regulations equivalent to a constitution of the governing body of international football.

The role of the national public authorities is essential, since there is a delegation of public service from the some member State to their national associations. In this case, the supervision made by public authorities must also include a support of those national associations to become more involved in the AML/CFT system.

Description of the risk scenario

As the most popular sport worldwide, football can be vulnerable to money laundering in the following main areas:

(1) Transfer of players,
(2) Investments in football clubs,
(3) Betting, and
(4) Sports competitions awarding.

The first document from the EU that recognised the importance of the sport was published in July 2007 (EU White Paper on Sport)[398]. 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[399]. This was followed by a resolution on 11 June 2015 on revelations on high-level corruption cases in FIFA[400] and a resolution on 2 February 2017 on an integrated approach to sport policy, covering good governance, accessibility and integrity[401]. 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 the Council of Europe Convention on the Manipulation of Sports Competitions[402]. 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 is fully effective 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.

---

[398] *White Paper on Sport*; European Commission, Brussels, 11.7.2007; COM(2007) 391 final.
[399] 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
[400] 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
[401] 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
[402] 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/manipulation-of-sports-competitions
The Convention entered into force on 1 September 2019. It has been ratified by Norway, Portugal, Ukraine, Moldova, Switzerland, Italy and Greece. It has been signed by 30 other European States and by Australia. https://www.coe.int/en/web/sport/manipulation-of-sports-competitions

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.

The impact of COVID-19

The Covid-19 pandemic has heightened several growing trends which could put the sector at greater risk. The pandemic has had a devastating effect on club finances. Many European clubs, especially at the lower end of the scale, have seen their revenue streams impacted severely. With the strain intensifying on many clubs to even stay solvent, the need and urgency for cash injections has also escalated. This scenario can often lead to less focus bring placed on the due diligence practices on potential investors and lower barriers to their entry.

Against this background UEFA identifies three specific trends which could lead to less transparency and, given the current economic climate, pose a greater risk to the sector (in terms of money laundering and integrity):

(1) Investment by private funds:

Private funds can pose a challenge to efforts in tracing individual investors or the money flows providing the equity. Whilst the entity / individuals managing the fund are visible, the identity of the investors into the fund can be opaque.

(2) Foreign owners:

Risk appears in those cases where investments originate from countries where the transparency of the level of investments and individuals' shareholdings is limited.

(3) Multi-club ownership:

Cases of individual parties owning or having stakes in more than one professional club can increase opportunities and risk of laundering; for example, via overvalued player transfer / loan deals between sister clubs, as well as multi-club commercial deals yielding revenues apportioned subjectively back to individual clubs.

Threat

Terrorist financing

The assessment of the terrorist financing (TF) threat arising from collecting and transferring 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.

Conclusions: 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[403].

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 poly-criminal 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 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

[403] A general introduction to money laundering in professional football as well as an overview of several high-profile cases are presented in Nelen, H., "Having the Blues: Money Laundering in Professional Football", *Contemporary Organised Crime. Developments, Challenges and Responses;* Studies of Organised Crime, vol. 18; Springer, Utrecht, 2020.

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.

Conclusions: 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.

Conclusions: 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.

Authorities and national associations must be particularly vigilant regarding the financing of clubs which call on international investors through complex legal arrangement, such as the use of loans endangering the financial balance of clubs.

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.

Conclusions: 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).

Risk level

As regards **terrorist financing**, the level of threat has been assessed as moderately significant (2), while the level of vulnerability has been assessed as moderately significant / significant (2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔ 1,6 – 2,5 Moderately significant MEDIUM

As regards **money laundering**, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as moderately significant / significant (2/3).

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

➔ 2,6 – 3,5 Significant HIGH

Conclusions: estimated risk level for terrorist financing is MEDIUM and for money laundering HIGH.

Mitigating measures

The European Parliament has urged Member States to create the crime of sporting fraud[404]. In addition, in 2014, the FIFA Executive Committee approved the Regulations on Working With Intermediaries[405].

The Annex to the Commission Decision adopting the Arrangement for Cooperation between the European Commission and the Union of the European Football Associations (UEFA)[406], 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 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;
- 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 havens. 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 and federations to comply, under penalty of sanctions, with the Registration of National or International Players Transfers. They must provide complete information about the

[404] 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

[405] https://www.fifa.com/about-fifa/who-we-are/news/fifa-executive-committee-approves-regulations-working-with-intermediarie-2301236

[406] European Commission, Brussels, 19.2.2018, C(2018) 876 final.

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[407];
- creating an obligation to conduct an independent audit in sports clubs and federations;
- considering the cross-border nature of ML and TF, Member States should seek international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

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;
- supervise agents' business practices by requiring certifications from accountancy professionals;
- 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.

[407] In this regard, the Council of Europe, based on the work of its Group of States against Corruption (GRECO), has recognised FIFA's ongoing efforts to reform the transfer system, stating that the soon-to-be-operational FIFA Clearing House "will represent a milestone in achieving comprehensiveness, transparency and integrity of the transfer system for football players around the world". The FIFA Football Agent Regulations are due to enter into force in July 2022
The Council of Europe's report *FIFA Transfer System Reform – Analysis and Recommendations*, of 7 June 2021, can be found at: https://rm.coe.int/eccd-bo-tp3-2021-fifa-transfer-system-recs/1680a2c2cd

FREE-TRADE ZONES

1. Free zones

Product

Free zones

Sector

Free-trade zones, Free zones — Customs, direct taxation

General description of the sector and related product/activity concerned

Free-trade zones (FTZs, also known as **free zones**) are 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 124 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 Financial Action Task Force (FATF) defines FTZs as 'designated areas within jurisdictions in which incentives are offered to support the development of exports, foreign direct investment (FDI), and local employment'[408].

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 a 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.

The Union Customs Code (UCC) also makes provision for free zones[409]. 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.

As regards direct personal taxation, free zones are considered to fall outside the normal national rules for direct taxation for non-resident customers, for example, capital gains taxes and wealth taxes, of the Member States where the free zone is established. In terms of business taxation, Member States can set up SEZs which have specific preferential business tax measures not available elsewhere in the respective Member State. In setting up such SEZs, Member States are required to comply with the EU's state-aid rules and the Code of Conduct on Business Taxation (which they have agreed to limit harmful tax practices)[410].

Goods held in free zones are subject to EU rules on value added tax (VAT), customs duties and excise duties. However, only when the goods are made available in the EU for sale or for private use or consumption are VAT and duties payable. Therefore, the longer the goods stay in free zones, the longer the payment of any duties and indirect taxes can be delayed.

---

[408] FATF, 'Money laundering vulnerabilities of Free Trade Zones', March 2010, available at: https://www.fatf-gafi.org/documents/documents/moneylaunderingvulnerabilitiesoffreetradezones.html

[409] 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*.

[410] 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.

Free ports

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 same tax and customs advantages as other free zones, and provide a high degree of secrecy.

In the EU

There are 78 free zones in the EU[411]. 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. It has only a few counterparts in the world, the most well-known located in Geneva, Monaco, Singapore, Beijing and Delaware (USA).

The other free zones are located in 20 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

Free zones are typically regarded as presenting high ML/TF risks[412]. Free zones offer a number of advantages from customs and taxation perspectives which may make them more likely to facilitate predicate offences or abuses[413]. Goods in the free zones are only subject to EU customs duties and indirect taxation if they are made available for sale in the Union market or for private use or consumption in the customs territory of the Union. There is no time limit on how long goods can be stored in a free zone, therefore, customs and taxes can be suspended or not paid at all, for example under capital gains tax, if the tax jurisdiction where the seller is resident is unaware of the sale. The misuse or the breach of VAT and custom duties rules undermine their collection and, as they are part of the EU's own resources, it will lead to losses of income for both the Member States and the Union's financial interests.

Free zones fall outside the national direct tax systems of the Member States. Council Directive 2011/16/EU on administrative cooperation in direct taxation[414] ('the DAC') does not contain provisions to automatically exchange information, including on beneficial ownership, between tax authorities on assets held in free zones[415]. This lack of information may make tax evasion more likely, for example, for taxes related to capital like capital gains, wealth taxes and inheritance taxes. In its 2021 report on the evaluation of the DAC, the European Parliament recommended that the scope of the DAC be extended to include non-financial assets such as cash, art, gold or other valuables held at free ports, custom warehouses or safe deposit boxes, and ownership of yachts and private jets[416].

Although the risks described above are applicable to all free zones and, to a lesser extent, customs warehouses[417], the risks are exacerbated in the case of high-value goods held in free ports. Pointing at the rapid growth in the high-end of the art market and the physical expansion of luxury storage spaces,

---

[411] 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/system/files/2020-04/list_freezones.pdf

[412] FATF, 'Money laundering vulnerabilities of Free Trade Zones', March 2010, available at: https://www.fatf-gafi.org/documents/documents/moneylaunderingvulnerabilitiesoffreetradezones.html

[413] http://coffers.eu/wp-content/uploads/2019/11/D4.7-Case-Study.pdf

[414] Council Directive 2011/16/EU of 15 February 2011 on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, *OJ L 64, 11.3.2011, p.1-12.*

[415] Under DAC5, Member States can request information from free zone operators, including information on beneficial ownership, however they must have a prior indication that the taxpayer is using the free zone in the first place.

[416] https://www.europarl.europa.eu/doceo/document/A-9-2021-0193_EN.html

[417] In contrast to free zones, a customs authorisation is required, security/guarantee for the goods must be provided and a customs declaration is needed.

a research paper suggests that luxury free ports are establishing themselves as new players in the global system of tax abuse[418].

The main issues encountered with free zones is the lack of transparency in terms of:

- Who owns what in free zones;
- The valuation of goods;
- The change of ownership of the goods stored there, and
- Any transformation of the goods in the free zone.

A Free Trade zone can facilitate **missing trader fraud**[419] in the EU. Criminal networks can incorporate companies in the FTZs, which can be used for customs and VAT frauds.

In the scenario of "cross invoicing," a company in a Member State involved in intracommunity trade would register domestic acquisitions of usually intangible goods from "missing traders" followed by exports outside the EU to offset the output VAT. The criminal networks can export intangible goods to a company incorporated in a FTZ, without involving the customs authorities. (It must be noted that, in this case, customs authorities ***should be involved***. If the goods are just taken out from the free zone without declaring them, i.e. without involving the customs authorities, this is due to an illegal activity, not to free zones themselves.)

Moreover, the criminal networks can use the FTZs in complex MTIC carousel frauds where the goods are imported in the EU from a FTZ, at a diminished value, traded in a chain of shell companies inside the EU, and subsequently re-exported at a significantly higher value, by a broker company which would receive VAT reimbursements from the state treasury. In contrast, the companies on the chain would have failed to account for their VAT obligations. Once outside the EU, the same goods can be traded between several companies and re-imported at the diminished value, and the criminal patter can be performed again.

In addition, a FTZ can be used to manipulate the customs value of goods before their importation in the EU. A trading activity between two companies incorporated in a FTZ can be done outside of the customs supervision; therefore, the value of the commodity can be diminished, resulting in less VAT and customs duties paid by the company performing the importation in the EU.

Lastly, the criminal networks can use companies from a FTZ to funnel the illicit proceeds from VAT frauds outside EU, by using fictitious trading agreements, orders and invoices to justify payments to non-EU countries.

A study of the facilitation of money laundering and terror finance through the trade of works of art by the US Department of the Treasury[420] notes that art storage facilities – often described as 'freeports' present money laundering vulnerabilities and can be used for illicit transactions.

In addition, free zones 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. In this regard, a 2018 study by the Organisation for Economic Cooperation and Development (OECD) and the EU Intellectual Property Office (EUIPO) found that

[418] Helgadóttir, O. (2020). The New Luxury Freeports: Offshore Storage, Tax Avoidance, and 'Invisible' Art. Environment and Planning A. https://doi.org/10.1177/0308518X20972712

[419] Missing trader fraud (also called missing trader intra-community fraud or MTIC fraud) involves the theft of Value Added Tax (VAT) from a government by fraudsters who exploit VAT rules, most commonly the European Union VAT rules which provide that the movement of goods between member states is VAT-free.

[420] Department of the Treasury, Study of the Facilitation of Money Laundering and Terror Finance through the Trade in Works of Art, February 2022, available at:
https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf

the establishment of an additional free trade zone within an economy was associated with a 5.9% increase in the value of exported counterfeit and pirated products[421]. As part of the broader efforts to counter illicit trade, in October 2019 the OECD Council issued a recommendation on enhancing transparency in free trade zones which also contains a code of conduct for clean free trade zones[422].

The European Parliament, in its Resolution of 26 March 2019 on financial crimes, tax evasion and tax avoidance[423] called on the Commission to bring forward a proposal for the urgent phasing out of the system of free ports in the EU[424]. The Parliament expressed its concern over various risks associated with free ports, including the possibility that they could be used for purposes of tax evasion or to achieve the same effects as tax havens[425].

According to a study by UNCTAD[426], there are more than 5,000 free zones worldwide and the number is expected to grow in the coming years. 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,
- intellectual property crimes,
- illegal tobacco trade[427],
- arms trafficking,
- illegal wildlife trade,
- tax evasion, and
- human-smuggling.

The World Customs Organisation's (WCO) analysis of 626 seizures between January 2011 and August 2018 demonstrates that drugs, counterfeit products, tobacco and arms represented respectively 23.5%, 22.8%, 9.9% and 2.7% of all seizures[428]. 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[429].

In most EU free zones 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 are 'obliged non-financial entities' as of 10 January 2020 onwards and therefore subject to the same customer due diligence (CDD) requirements as, for example, real-estate agents and notaries.

---

[421] OECD/EUIPO (2018), 'Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends', OECD Publishing, Paris/EUIPO, page 13.
[422] OECD, Recommendation of the Council on Countering Illicit Trade: Enhancing Transparency in Free Trade Zones, adopted on 21 October 2019, available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0454#dates
[423] European Parliament resolution of 26 March 2019 on financial crimes, tax evasion and tax avoidance (2018/2121(INI)), available at: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0240_EN.pdf
[424] Ibid, para 211.
[425] Ibid, para 204.
[426] François Bost, (2019), "Special economic zones: methodological issues and definition", UNCTAD Transnational Corporations Journal, available at: https://unctad.org/system/files/official-document/diaeia2019d2a7_en.pdf
[427] Europol Financial Intelligence Public Private Partnership (EFIPPP) information: regarding the illegal trade of tobacco, large-scale international smuggling continues with free trade zones playing an important role as transit hubs where illicit tobacco is moved using shipping containers under the disguise of cover loads.
[428] World Customs Organization, "'Extraterritoriality' of Free Zones: The Necessity for Enhanced Customs Involvement", WCO Research Paper No. 47, available at: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/research-paper-series/47_free_zones_customs_involvement_omi_en.pdf?la=en
[429] In June 2020 Europol and EUIPO published a report, in the form of a case book, to inform law enforcement officials and policy makers about the various ways in which IP crime is linked to other forms of criminal activity: https://www.europol.europa.eu/publications-documents/ip-crime-and-its-link-to-other-serious-crimes-focus-poly-criminality

They have also taken on the role of anti-money laundering (AML) gatekeepers, as they have to report suspicious transactions to Financial Intelligence Units (FIUs).

Due to privacy and confidentiality clauses (akin to bank secrecy), owners of free zones do not disclose the value of goods stored on their premises, as declared by customers, so it is impossible to give estimates of the value of the stored goods worldwide. One of the very few estimations comes from the Swiss government, which in 2016 estimated that the country's free ports held around EUR 100 billion in valuables[430].

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[431]. Free zones are also perceived as facilities that protect their clients' identity and financial dealings, much as private banks used to.

Terrorist financing

Free zones 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 zones 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 as 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[432]. Money laundering in free zones can also involve misrepresentation of the price, quantity or quality of goods, including intangible ones, thus giving rise to risks linked to trade-based money laundering (TBML)[433].

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

[430] https://www.finews.com/news/english-news/23238-swiss-freeports-move-to-crack-down-on-art,-loot
[431] FATF, "Money-laundering vulnerabilities of free-trade zones", March 2010, available at: http://www.fatfgafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf
[432] Although shipment of counterfeit goods to the EU still occurs largely in bulk by freight transport, in recent years there has been a strong increase in express transport. This sharp growth in trade via small parcels is related to the growth in online marketplaces selling counterfeit goods. New land routes that have opened in recent years, in particular the growing number of rail connections between China and the EU, may provide counterfeiters with the possibility of diversifying their routes and transportation methods: https://www.europol.europa.eu/newsroom/news/new-threat-assessment-confirms-links-between-counterfeiting-and-organised-crime-in-eu
[433] A. Moiseienko, A. Reid, I. Chase, *Improving Governance and Tackling Crime in Free-Trade Zones*, RUSI, October 2020, p. 14.

- cooperating with transport companies and distributors.

Recent case illustrating the *modus operandi*:

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. Before the leak, he stated that he was not the owner of the painting[434].

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 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.

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[435].

The report gives an example of a EUR 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.

A long-running court case, also referred to as the 'Bouvier affair' whereby an art shipper and dealer was accused by a Russian oligarch of swindling USD 1 billion over a 10 year period. The story shone a light on the world of free ports as the Geneva Freeport was where Bouvier's moving and storage company was the largest tenant.

In 2016, a junket operator licensed in First Cagayan Special Economic Zone (the Philippines) played a main role in transferring funds (totalling 101 million US dollars) stolen from the from bank accounts of the Bangladesh National Bank held in the New York's Federal Reserve[436].

In 2018, Organized Crime and Corruption Reporting Project described the following *modus operandi* of Albanian organized crime groups that use the free trade zones for cigarette smuggling. Criminal gangs have dozens of trading houses legally buying tax-free cigarettes for free trade zones buy extra boxes of cigarettes in each shipment. Gangs buy the extra cigarettes and combine the surplus into one shipment, that gets smuggled into European ports. The cigarettes are then sold around Europe[437].

In 2019, the United Nations Offices on Drugs and Crime (UNODC) stated that free trade zones and special economic zones in Laos and Myanmar have become major gambling centres and have been identified as key players in the illicit trade of drugs, precursors and wildlife products[438].

Conclusions: The ML threat relating to free zones is considered significant (level 3).

[434] https://www.artlyst.com/news/nahmad-family-setback-25m-modigliani-painting-nazi-restitution-case/
[435] http://www.fatf-gafi.org/media/fatf/documents/reports/ML-TF-through-trade-in-diamonds.pdf
[436] 'Free For All Zone' - Free Trade & Special Economic Zones (FTZ & SEZ) International Online Betting Operators & Gambling, 5th OECD Task Force or Countering Illicit Trade, GOV/PGC/HLRF/TFCIT/RD(2017)3, 27 March 2017, pp. 9-10.
[437] https://www.occrp.org/en/goldensands/free-zones
[438] UNODC, "Transnational Organised Crime in Southeast Asia: Evolution, Growth and Impact", 2019, available at: https://www.unodc.org/documents/southeastasiaandpacific/Publications/2019/SEA_TOCTA_2019_web.pdf

Vulnerability

Terrorist financing

The assessment of TF vulnerability relating to free zones shows that:

a) risk exposure

Free zones 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 the 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 zones or under customs warehousing procedures are technically 'in transit', even though there are no time limits in most free zones of this kind. Goods can enter a free zone, 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 zones. 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

Risk awareness is still developing, following the designation of free port operators as obliged non-financial entities in AMLD5. 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, especially since so far free ports have been attractive to some clients precisely because they allowed shielding their ownership of goods.

Another barrier to developing more risk awareness among national authorities is that one of the reasons why jurisdictions create free ports is to boost trade and investment by providing a liberalised regulatory regime. Ensuring that free ports are not used for criminal activities may be a secondary objective, especially if the goods stored and processed in a free port never enter the host country. This often leads to prioritising revenue-generating activities over those aimed at tackling ML/TF risks and lack of clear allocation of responsibility and accountability for crime prevention[439].

Level of awareness among financial institutions could further benefit from more guidelines and education on the nature of free trade zones and the criminal risks associated with them[440].

c) legal framework and control

As they are subject to EU and national AML regulations (as long as they are involved in the trade in works of art), free zones 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.

[439] A. Moiseienko, A. Reid, I. Chase, *Improving Governance and Tackling Crime in Free-Trade Zones*, RUSI, October 2020, p. 22.
[440] Ibid., p. 44

Conclusions: When used anonymously, free zones 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 zones 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 money laundering cases detected and addressed by LEAs calls for specific consideration.

In addition, large international flows characteristic for free ports may expose them to money laundering activities from other countries.[441] Free ports offering their storage services to banks (for example for storing gold), such as the Luxembourg free port, are also exposed to second-order risks.[442]

Conclusions: Free zones 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 zones is therefore considered very significant (level 4).

Risk level

As regards terrorist financing, both the level of threat and the level of vulnerability have been assessed as significant (3).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
➔	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

As regards money laundering, the level of threat has been assessed as significant (3), while the level of vulnerability has been assessed as very significant (4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is HIGH and for money laundering VERY HIGH.

Mitigating measures

There is scope to improve the regulation of EU free zones.

- Following the findings and proposed mitigating measures of the 2019 Supranational Risk Assessment[443], the proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[444], adopted in July 2021, clarified the scope of the entities subject to the obligation[445]. Pursuant to the changes, the phrase "free

[441] National Risk Assessment Of Money Laundering And Terrorist Financing, Luxembourg, 15th September 2020, p. 122
[442] Ibid.
[443] 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, p. 247.
[444] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Brussels, 20.7.2021, COM(2021) 420 final, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:0a4db7d6-eace-11eb-93a8-01aa75ed71a1.0001.02/DOC_1&format=PDF
[445] The main clarification being that customs warehouses are now explicitly included with regard to dealing in art.

ports" was substituted with the term **"free zone"**, and it was clarified that customs warehouses are also an obliged entity within the meaning of Article 3 of the proposal for a new Regulation. These changes align the language of the AML/CFT framework with the Union Customs Code (UCC). The proposal is at present undergoing inter-institutional negotiations.

- In 2022, the Commission will undertake an evaluation of EU free zones. This evaluation will include an assessment of the benefits of free zones as well as the costs of free zones, including the risk of possible misuse of free zones, both in the customs and taxation area. Currently there is lack of information available on the activities in Free zones so the evaluation will focus on data collection and it will also determine among others whether the Commission should work on a change in the customs legislation on free zones. The evaluation will gather information on the following:
    - Are free zones subject to national AML/CFT requirements?
    - Do national tax authorities have access to information on goods held in free zones and under which circumstances, including any automatic exchange of information provisions?
    - What information is contained in the free zone asset registers, including information on beneficial ownership of assets held through legal persons and legal arrangements?
    - What controls are in place to ensure proper segregation of goods held for an EU customer and goods held for export to ensure correct customs duties and taxes are levied, including possible cases of processing of goods?
    - What is the volume of activities in free zones and can and do all free zones store high-value goods?

The Member States should:

- Carry out regular independent AML/CFT audits of free trade zone operators' compliance functions and ensure adequate and consistent enforcement of the AML/CFT procedures and oversight already enshrined in law.
- Ensure that free trade zones operators regularly share information with the relevant AML/CFT authorities on UBOs and changes in the ownership of free port assets.
- Assess the ML/TF risks associated with the free zones, operating in their territories, as part of their national risk assessments.
- 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.
- Considering the cross-border nature of ML and TF, Member States should seek for international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol.

CITIZENSHIP/RESIDENCE

1. Investor citizenship and investor residence schemes

Product

Investor citizenship schemes and investor residence schemes

Sector

Citizenship/residence

General description of the sector and related product/activity concerned

Investor citizenship and investor residence schemes aim to attract investment in a particular country by granting investors citizenship or residence rights in exchange for investments in the country concerned. Such schemes have raised serious concerns about certain inherent risks, in particular as regards security, money laundering, tax evasion/avoidance[446] and corruption.

Investor citizenship schemes are often referred to as 'citizenship investment programmes' ('CIPs'), 'citizenships for sale' or 'golden passports'. They allow foreigners to obtain the nationality of a country in return for a pre-determined payment or investment. Criteria that apply to the ordinary naturalisation procedure, such as a certain period of legal presence in the country, are usually waived. 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 aims of these programmes are economic enrichment and diversification for the country operating the scheme[447], there are reported instances of their abuse, posing risks for the Member States and the Union as a whole, including in terms of security, money laundering, corruption, circumvention of EU rules and tax evasion[448].

The benefits of such schemes 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. For example, many countries operating investor citizenship schemes 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.

[446] 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.

[447] 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.

[448] 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 EU', Brussels, 23.1.2019, COM(2019) 12 final, available at: https://ec.europa.eu/info/files/report-commission-european-parliament-council-european-economic-and-social-committee-and-committee-regions-investor-citizenship-and-residence-schemes-european-union_en

Description of the sector

In the EU, only Malta[449] still operates investor citizenship schemes. Due to the nature of EU citizenship, such schemes have implications for the Union as a whole. When a Member State awards nationality, the person concerned automatically becomes an EU citizen and enjoys all rights linked to this status, such as the right to move, reside and work freely within the EU, or the right to vote in elections for the European Parliament. They may also be used to circumvent certain nationality requirements in EU law[450]. As a consequence, the effects of investor citizenship schemes are neither limited to the Member States operating them, nor are they neutral with regard to other Member States and the EU as a whole. Indeed, although these are national schemes, they are deliberately marketed and often explicitly advertised as a means of acquiring EU citizenship and the rights and privileges associated with it. Until recently, Cyprus was also operating an investor citizenship scheme. However, following revelations about potential serious abuses[451], Cyprus suspended its citizenship investment programme on 1 November 2020[452], while continuing to process pending applications. An official inquiry found that the Cypriot authorities had broken the law on numerous occasions, with more than half of the naturalisations granted illegally[453].

On 20 October 2020, the Commission launched infringement procedures against Cyprus and Malta regarding their investor citizenship schemes[454]. On 9 June 2021, the Commission took further steps in the infringement procedures[455]. The Commission considers that by establishing and operating investor citizenship schemes that offer citizenship in exchange for pre-determined payments and investments, these two Member States fail to fulfil their obligations under the principle of sincere cooperation (Article 4(3) TEU) and the definition of citizenship of the Union as laid down in the Treaties (Article 20 TFEU). The Commission is in dialogue with Bulgaria, given similar concerns regarding Bulgaria's investor citizenship scheme.

Investor residence schemes exist in 19 EU Member States[456]: Bulgaria, Czechia, Estonia, Ireland, Greece, Spain, France, Croatia, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania and Slovakia. The risks inherent in such schemes are similar to those raised by investor citizenship schemes, as confirmed by the Commission's report on investor citizenship and residence schemes in the EU, published in January 2019. 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.

In its 2020 citizenship report[457], the Commission stressed that the integrity of EU citizenship is undermined when Member States grant nationality and, hence, EU citizenship, without any requirement for a real link between the country and the investor. The report also highlights that citizenship

[449] Bulgaria closed its citizenship by investment programme in March 2022. Also in March 2022 Malta suspended its scheme for Russian and Belarusian citizens. Cyprus already stopped its controversial citizenship for investment programme in 2020.
[450] Regulation (EC) 1008/2008 on common rules for the operation of air services in the Community; *OJ L 293, 31.10.2008, p. 3.*
[451] See 'The Cyprus Papers', available at: https://interactive.aljazeera.com/aje/2020/cyprus-papers/index.html and the 'Cyprus Papers Undercover', available at: https://www.aljazeera.com/news/2020/10/12/cypriot-politicians-implicated-in-plan-to-sell-criminals-passport
[452] For more information: https://www.reuters.com/article/cyprus-citizenship-int-idUSKBN26Y17D
[453] For more information: https://www.reuters.com/world/europe/cyprus-government-broke-its-own-laws-granting-passports-inquiry-2021-06-07/
[454] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1925
[455] https://ec.europa.eu/commission/presscorner/detail/en/inf_21_2743
[456] The two lists overlap, as two countries — Bulgaria and Malta — trade with both.
[457] EU Citizenship Report 2020: Empowering Citizens and Protecting Their Rights. Available at: https://ec.europa.eu/info/files/eu-citizenship-report-2020-empowering-citizens-and-protecting-their-rights_en

investment schemes facilitate money laundering, tax evasion and corruption, a concern also raised by the Commission's 2019 report on investor citizenship and residence schemes in the EU[458].

On 20 October 2020, the Commission launched infringement procedures against Cyprus and Malta regarding their investor citizenship schemes[459]. On 28 March 2022 the Commission urged Member States to act on 'golden passports' and 'golden residence permits' schemes, and to take immediate steps in the context of the Russian invasion of Ukraine[460].

The European Parliament, in its Resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing,[461] called on the Member States to phase out all existing citizenship by investment or residency by investment schemes as soon as possible, particularly when there is insufficient verification and lack of transparency, in order to minimise the often linked threat of money laundering, the undermining of mutual trust and the integrity of the Schengen area, in addition to other political, economic and security risks to the EU and its Member States. Furthermore, in its Resolution of 17 December 2020 on the EU Security Union Strategy, the European Parliament recalled that Member States with residence and citizenship by investment schemes often facilitate corruption and money laundering, thereby importing security risks into the Union. In February 2022, a report from the European Parliament[462] called for the EU to ban the sale of citizenship by investment schemes and to regulate residence by investment schemes.

The 2019 Commission's report also highlighted that 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. In order to address these risks, the Commission adopted on 27 April 2022 a proposal to recast the Long-Term Residents Directive[463], which includes rules to prevent that third-country nationals abusively acquire the EU long-term resident status on the basis of an investment. As such, it proposes, among other things, to include a provision to strengthen checks on the residence requirement, with particular regard to applications for EU long-term resident status submitted by investors.

Civil society has also strongly criticised investor schemes[464].

Investor citizenship schemes in third countries with visa-free access to the EU have increased in recent years, in particular in the Caribbean (Antigua and Barbuda, Dominica, Grenada, Saint Kitts and Nevis, Saint Lucia) and in the Pacific (Vanuatu). The government of the Solomon Islands has also announced plans to set up a similar programme, although it has not gone forward for the moment. Tuvalu has abandoned its plans for a scheme following EU concerns.

---

[458] 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 EU', Brussels, 23.1.2019, COM(2019) 12 final, available at: https://ec.europa.eu/info/files/report-commission-european-parliament-council-european-economic-and-social-committee-and-committee-regions-investor-citizenship-and-residence-schemes-european-union_en

[459] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1925

[460] Commission Recommendation of 28.3.2022 on immediate steps in the context of the Russian invasion of Ukraine in relation to investor citizenship schemes and investor residence schemes, C(2022) 2028 final: https://ec.europa.eu/home-affairs/recommendation-limit-access-individuals-connected-russian-belarusian-government-citizenship_en

[461] European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments (2020/2686(RSP)), available at: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204_EN.pdf

[462] Report with proposals to the Commission on citizenship and residence by investment schemes (2021/2026(INL)), Committee on Civil Liberties, Justice and Home Affairs, A9-0028/2022, 16.2.2022: https://www.europarl.europa.eu/doceo/document/A-9-2022-0028_EN.pdf

[463] COM(2022) 650 final.

[464] For more information: Transparency International/Global Witness, European Getaway — Inside the Murky World of Golden Visas, October 2018, https://www.transparency.org/whatwedo/publication/golden_visas and Global Witness, Europe's Golden Doors – Lack of Progress in stopping the criminal and corrupt accessing Europe via golden passports and visas, March 2020, https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/europes-golden-doors/

As regards visa-free candidate countries in the EU neighbourhood, Montenegro is currently running an investor citizenship scheme (to be phased-out following EU concerns), North Macedonia is increasingly granting citizenship to investors and Albania has announced plans to set up an investor citizenship scheme. In the Eastern Partnership, Moldova's scheme was first suspended following concerns by the EU and has now been recently terminated.

Most third countries concerned advertise the programmes as a way to obtain visa-free access to the EU quickly (i.e. circumventing the Schengen visa procedures and the in-depth risk assessment it entails).

Threat

Third-country nationals may invest in a Member State for legitimate reasons[465], 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[466], 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 are also concerns 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[467]. Furthermore, the procedure for screening applicants can be outsourced to private companies, where there is a permanent risk of conflict of interests and corruption.

It is important to highlight that the Commission's proposal for a Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[468] includes into the list of obliged entities operators involved on behalf of third country nationals in the context of investor residence schemes, thus subjecting them to AML/CFT obligations such as the carrying out of customer due diligence and reporting of suspicious transactions and activities[469]. The Commission did not propose to regulate actors involved in investor citizenship schemes given its concerns regarding the incompatibility of such schemes with EU law.

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[470], information for tax purposes could be sent to the wrong jurisdiction of residence. At international level, the OECD monitors investor citizenship and investor residence schemes which can potentially be misused or abused to misrepresent an individual's jurisdiction(s) of tax residence and

[465] 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.
[466] Europol Financial Intelligence Public Private Partnership (EFIPPP) information: OCGs exploit the loopholes provided by some 'Golden Visas' schemes to infiltrate in businesses/the legal economy. Golden visas/citizenship by investment in the particular jurisdiction, is a geographical indicator to determine the level of vulnerability to infiltration.
[467] The Guardian's 2021 investigation into the Maltese citizenship scheme for investment scheme and Al Jazeera's 2020 investigation into the Cypriot scheme are good examples in this regard.
[468] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Brussels, 20.7.2021, COM(2021) 420 final.
[469] The Commission considers that investor citizenship schemes, that is, schemes that offer citizenship of a Member State in exchange for pre-determined payments and investments, do not comply with the principle of sincere cooperation (Article 4(3) TEU) and the fundamental status of citizenship of the Union as laid down in the Treaties (Article 20 TFEU). As a consequence, the Commission does not propose to regulate such schemes.
[470] Within the EU Council Directive 2014/107/EU on the automatic exchange of financial account information, and at international level the OECD Common Reporting Standard on automatic exchange of financial account information.

endanger the proper operation of the common reporting standard's ('CRS') due diligence procedures[471]. Financial institutions are asked to take into account the OECD's assessment for customer due diligence procedures for the CRS.

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.

The 2019 Commission's report on investor citizenship and residence schemes in the EU also alerted that citizenship schemes run by third countries with visa-free access to the EU could be used to circumvent the Schengen visa procedure and the in-depth risk assessment it entails.

Terrorist financing

The assessment of the terrorist financing threat related to investor citizenship and residence schemes 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 discretion in the way that Member States approach security concerns beyond these checks.

Lack of transparency: The Commission's 2019 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 investor citizenship and investor residence schemes is considered as significant/very significant (level 3/4).

Money laundering

Examples of jurisdictions that have attracted wealthy people involved in money laundering schemes:

The 'Cyprus Papers' investigation by Al Jazeera revealed that Cyprus has become a financial refuge for rich Russian, Chinese, Ukrainian and Lebanese citizens and a hub for money laundering operations. Investigative journalists from Al Jazeera revealed that an investment of at least EUR 2.15 million in Cyprus has secured Cypriot and, thereby, EU citizenship for 1,400 wealthy individuals between 2017 and 2019. Some include family members, which brought the total number of individuals granted EU citizenship to nearly 2,500. Allegedly, among the primary applicants were individuals facing criminal charges or with prior convictions as well as 40 politically exposed persons (PEPs).[472] Moreover, earlier investigations by Reuters[473], Politis News[474] and the Organised Crime and Corruption Reporting

[471] For more information: https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/residence-citizenship-by-investment/

[472] The investigation by the Al-Jazeera allegedly found that the Republic of Cyprus provided citizenship through the CIP to several people linked to crime and corruption.

[473] For more information: https://www.reuters.com/investigates/special-report/cambodia-hunsen-wealth/

[474] For more information: https://politis.com.cy/politis-news/kypros/kypriako-diavatirio-ston-jho-taek-low-isos-o-pleon-katazitoymenos-epicheirimatias-ston-planiti/

Project[475] alleged that relatives of Cambodia's rulers and the Malaysian 1MDB fugitive financier Jho Low have obtained EU citizenship via the Cypriot citizenship investment scheme. 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. MONEYVAL also criticised the Cypriot investment programme as being vulnerable for abuse for money laundering purposes[476]. As already noted, Cyprus suspended its investor citizenship scheme in November 2020.

Maltese citizenship is similarly popular with wealthy third-country nationals. Several 'new' Maltese citizens have recently been charged with various criminal offences. For example, an Israeli citizen[477] who bought Maltese passports for himself and his family, and a Chinese billionaire[478] with Maltese passport, were charged respectively with fraud and aluminium tariff evasion in the US in 2019. Furthermore, a Russian national with Maltese citizenship, was suspected by Finnish authorities to be involved in an international money laundering scheme[479].

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.

Investor schemes 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 investor citizenship schemes; this has given rise to the risk of sanctions evasion in addition to the potential laundering of illicit funds. The Al Jazeera investigation into the Cypriot investor citizenship scheme, for example, revealed several Russian nationals on US or EU sanctions lists who allegedly obtained Cypriot citizenship.

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.

In August 2021, a Syrian national had his approval for citizenship revoked by the authorities of Vanuatu, after investigators found out the US government had placed sanctions against his businesses. According to the head of Vanuatu's Citizenship Commission other individuals are being investigated over concerns that international criminals are buying Vanuatu passports.

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

---

[475] For more information: https://www.occrp.org/en/daily/11047-malaysian-1mdb-fugitive-became-cypriot-citizen-in-2015 and https://www.occrp.org/en/investigations/a-key-player-in-malaysias-biggest-ever-corruption-scandal-found-sanctuary-in-cyprus-with-help-from-a-major-london-firm

[476] MONEYVAL, Council of Europe, Anti-money laundering and counter-terrorist financing measures Cyprus, Fifth Round Mutual Evaluation Report (MONEYVAL(2019)27), December 2019. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Cyprus.pdf

[477] https://www.sec.gov/litigation/litreleases/2019/lr24505.htm. and https://theshiftnews.com/2019/10/18/fifth-malta-cash-for-passports-client-charged-with-financial-crime-this-year/

[478] For more information: https://timesofmalta.com/articles/view/chinese-billionaire-with-maltese-passport-indicted-in-us.726178 and https://www.ft.com/content/7a7db298-b3af-11e9-8cb2-799a3a8cf37b

[479] For more information: https://lovinmalta.com/news/news-international/russian-man-with-maltese-passport-at-centre-of-10-million-european-money-laundering-scheme/

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 assigned 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 been subjected to greater scrutiny due to underlying circumstances.

Conclusions: In the light of the scenario described above, the level of the money laundering threat related to investor citizenship and investor residence schemes is considered as very significant (level 4).

Vulnerability

Terrorist financing

The assessment of the terrorist financing vulnerability related to investor citizenship and investor residence schemes 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. On security, it has been found that checks run on applicants are not always sufficiently robust.

On transparency, 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 appear to not exchange information on applicants for such schemes, nor do they inform each other of rejected applicants.

b) Risk awareness

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 discretion in the way that Member States address security concerns beyond these checks.

Conclusions: In this context, the level of terrorist financing vulnerability related to investor citizenship and investor residence schemes 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 investor citizenship and investor residence schemes is considered as very significant (level 4).

Risk level

As regards terrorist financing, both the levels of threat and vulnerability have been assessed as significant/very significant (level 3/4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
➔	2,6 – 3,5	Significant HIGH
	3,6 – 4	Very significant VERY HIGH

As regards money laundering, both the levels of threat and vulnerability have been assessed as very significant (level 4).

	RISK	
	1 – 1,5	Lowly significant LOW
	1,6 – 2,5	Moderately significant MEDIUM
	2,6 – 3,5	Significant HIGH
➔	3,6 – 4	Very significant VERY HIGH

Conclusions: estimated risk level for terrorist financing is HIGH and for money laundering VERY HIGH.

Mitigating measures

The citizenship schemes described have implications for the entire EU 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.

Similar risks exist for investor residence schemes, although the rights granted to residents are not the same as those acquired when becoming a citizen. A valid EU residence permit grants certain rights to third-country nationals to travel freely in the Schengen area.

For the Commission:

The Commission will continue to **monitor wider issues of compliance with EU law** raised by investor citizenship and residence schemes and will take necessary action as appropriate, in particular regarding:

- compliance of investor citizenship schemes resulting in the acquisition of EU citizenship in exchange for pre-determined payments and investment with EU law;
- systematic compliance with all obligatory border and security checks;
- Directive 2018/822/EU[480] which requires intermediaries to submit information on reportable cross-border tax arrangements to their national authorities[481] and which came into effect in 2020;
- the monitoring of the impact of investor citizenship and investor residence schemes implemented by visa-free countries as part of the visa-suspension mechanism;
- the monitoring of investor citizenship schemes in the context of the EU accession process.

[480] 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.*

[481] 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

The Commission continues to monitor closely investor citizenship and investor residence schemes in third countries whose nationals have visa-free access to the EU and to raise the issue in bilateral meetings with relevant stakeholders from the countries concerned. As regards countries in the Western Balkans and Eastern Partnership, the Commission also monitors investor citizenship schemes in the context of the visa suspension mechanism and the EU accession process.

As stated in the 2019 report, third countries enjoying visa-free status must carry out security and background checks of applicants for citizenship schemes to the highest possible standards; any failures in this regard could be grounds for re-imposing a visa requirement and suspending or terminating visa waiver agreement.

For the Member States:

The Commission considers that any investor citizenship scheme operated by the Member States resulting in the acquisition of EU citizenship in exchange for pre-determined payments and investments **should be phased out[482].**

With regard to investor residence schemes, Member States should ensure transparency and good governance in their implementation, with a view to addressing in particular risks of security, including 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 residence permits granted and rejected – alongside the 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 annual audit exercises to assess the implementation of the risk management plan;
- 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[483]), 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;
- considering the cross-border nature of ML and TF, Member States should seek for international cooperation and encourage relevant authorities in charge of preventing and combatting ML and TF to request support from agencies such as Europol, where relevant.

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.

[482] Reference must be made to the 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 EU', 23.1.2019, COM(2019) 12 final: https://ec.europa.eu/info/files/report-commission-european-parliament-council-european-economic-and-social-committee-and-committee-regions-investor-citizenship-and-residence-schemes-european-union_en

[483] https://ec.europa.eu/taxation_customs/business/tax-cooperation-control/administrative-cooperation/enhanced-administrative-cooperation-field-direct-taxation_en

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' beneficial 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.

Risk matrix by product/sector – comparative table 2017-2019-2022

SECTOR/PRODUCT	2017		2019		2022	
	TF residual risk	*ML residual risk*	*TF residual risk (shift)*	*ML residual risk (shift)*	*TF residual risk (shift)*	*ML residual risk (shift)*
Cash-related products						
1. Cash couriers	4,00	4,00	4,00	4,00	4,00	4,00
2. Cash intensive business	3,20	3,60	3,20	3,60	3,20	3,60
3. High value banknotes	3,20	4,00	3,20	4,00	3,20	4,00
4. Payments in cash	4,00	4,00	4,00	4,00	4,00	4,00
5. Privately owned ATMs			4,00	4,00	4,00	4,00
Financial sector						
1. Retail banking sector (formerly "Deposits on accounts")	2,80	2,80	3,40 (+0,60)	3,40 (+0,60)	3,20 (-0,20)	3,40
2. Retail and Institutional investment sector (formerly "Institutional investment sector — Banking")	2,00	2,00	1,00 (-1)	3,00 (+1)	0,80 (-0,20)	2,70 (-0,30)
Institutional investment sector — Brokers (discontinued *fiche*, now treated within the above one)	2,60	2,60	1,00 (-1,60)	3,00 (+0,40)		
3. Corporate banking sector	2,40	2,40	1,00 (-1,40)	3,00 (+0.60)	1,00	2,70 (-0,30)
4. Private banking sector	0,00	3,00	0,00	4,00 (+1)	0,00	3,50 (-0,50)
5. Crowdfunding	2,60	2,60	2,00 (-0,60)	2,00 (-0,60)	2,00	2,00
6. Currency exchange	3,00	3,00	3,00	3,00	3,00	3,00
7. E-money	4,00	3,40	3,00 (-1)	3,00 (-0,40)	3,00	3,00
8. Transfers of funds and money remittance (formerly "Transfers of funds")	4,00	4,00	4,00	3,40 (-0,60)	4,00	3,40
9. Illegal transfers of funds — Hawala	2,00	2,00				
10. Payment services	2,40	2,80	3,00 (+0,60)	3,00 (+0,20)	3,00	3,00
11. Crypto-assets (formerly "Virtual currencies and other virtual assets")	3,20	3,20	3,00 (-0,20)	3,00 (-0,20)	4,00 (+1)	4,00 (+1)
12. Business loans	1,00	1,00	1,00	2,00 (+1)	1,00	2,00
13. Consumer credit and low-value loans	3,00	0,00	3,00	2,00 (+2)	3,00	2,00
14. Mortgage credit and high-value asset-backed credits	1,60	2,40	1,00 (-0,60)	2,40	1,00	2,40
15. Life insurance	2,00	2,00	2,00	2,00	1,70 (-0,30)	1,70 (-0,30)
16. Non-life insurance	2,00	1,00	2,00	1,00	1,60 (-0,40)	1,00
17. Safe custody services	0,00	3,00	0,00	3,00	0,00	2,70 (-0,30)
Non-financial sector						
Creation of legal entities and legal arrangements	3,20	4,00	3,20	4,00		
Business activity of legal entities and legal arrangements	2,60	3,40	2,60	3,40		
Termination of legal entities and legal arrangements	2,00	2,00	2,00	2,00		
The previous 3 *fiches* have been discontinued. The areas covered by them are now treated under the next 3 ones:						
1. Trusts					2,40	4,20

2.	Nominees					2,00	4,00
3.	Companies					2,50	4,00
4.	High value goods – artefacts and antiquities	3,20	3,20	3,20	3,20	3,20	3,20
5.	High value assets – Precious metals and precious stones	3,00	3,40	3,00	3,40	3,00	3,40
6.	High value assets – other than precious metals and stones	0,00	3,40	0,00	3,40	0,00	3,40
7.	Couriers in precious metals and stones	3,20	3,60	3,20	3,60	3,20	3,60
8.	Investment real estate	4,00	4,00	4,00	4,00	4,00	4,00
9.	Services provided by accountants, auditors, advisors, and tax advisors	3,40	3,40	3,40	3,40	3,40	3,00 (-0,40)
10.	Legal services from notaries and other independent legal professionals *(notaries)*	3,40	3,40	3,40	3,40	3,40 *3,10*	3,40 *3,10*
Gambling							
1.	Betting	0,00	3,00	0,00	3,00	0,00	3,00
2.	Bingo	0,00	1,00	0,00	1,00	0,00	1,00
3.	Casinos	0,00	2,80	0,00	3,00 (+0,20)	0,00	2,00 (-1)
4.	Gaming machines (outside casinos)	0,00	2,00	0,00	2,00	0,00	2,00
5.	Lotteries	0,00	2,00	0,00	2,00	0,00	2,00
6.	Poker	0,00	3,00	0,00	3,00	0,00	3,00
7.	Online gambling	0,00	3,00	0,00	2,00	4,00 (+4)	4,00 (+2)
Non-Profit Organisations (NPO)							
1.	Collection and transfers of funds through a NPO *(funding by EU or Member States)*	3,00 *2,00*	3,00 *2,00*	2,40 (-0,60) *1,00* (-1)	2,00 (-1) *1,00* (-1)	2,40 *1,00*	2,00 *1,00*
Professional sports							
1.	Investments in professional football and transfer agreements			2,30	2,70	2,30	2,70
Free-Trade Zones							
1.	Free zones			3,00	3,60	3,00	3,60
Citizenship-Residence							
1.	Citizenship investment programmes and investor residence schemes			3,50	3,80	3,50	3,80

ANNEX II

METHODOLOGY FOR ASSESSING MONEY LAUNDERING AND TERRORIST FINANCING RISKS AFFECTING THE INTERNAL MARKET AND RELATED TO CROSS-BORDER ACTIVITIES

The methodology described below was approved at the ISG AML/CF of 4 November 2015 and has been used for the Supra-National Risk Assessments of 2017, 2019, and 2022.

For the purposes of assessing ML/TF risk at the supra-national level, the following key concept of risk is being followed:

A risk means the ability of a threat to exploit the vulnerability of a sector for the purpose of money laundering or terrorist financing. A risk falls within the scope of this assessment as soon as it affects the internal market because of its characteristics – whatever the number of Member States concerned (i.e. even if it may concern only one Member State). The scope covers both known and emerging risks – i.e. whether the risk materialised or not.

1. INTRODUCTION

The Financial Action Task Force (FATF) recommends that countries shall consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of each sector submitted to AML/CFT requirements when they decide to conduct a risk assessment. Money laundering (ML) and terrorist financing (TF) risks shall be identified, assessed and understood, and measures to prevent ML/TF shall be commensurate with the risks identified.

On the basis of these recommendations, the Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing[484] recognises the importance of a **supranational approach to risk identification.** It tasks the Commission to conduct the review of specific risks that could arise at European level and could affect the internal market ("supranational risk"). The Commission shall therefore conduct such Supranational Risk Assessment on money laundering and terrorist financing ("SNRA"). A risk identification is also conducted **at national level** by each Member States so that to ensure proper risk identification and risk mitigation of national specific risks. A third layer of risk identification is provided **by sectors themselves**, taking into account risk factors including those relating to their customers, countries, products, services, transactions or delivery channels.

These three layers of risk assessments (and where appropriate risk mitigation) allow building a comprehensive awareness and analysis of ML/TF risks in the European Union. There are complementary and have the same level of relevance as regards, respectively, the sectorial, national and supranational approach to the risk assessment.

Even though national and sectorial risk assessments, among other sources, may prove to be essential building blocks for the SNRA conducted by the Commission, it cannot be considered as a mere compilation of these ones. The SNRA exercise shall therefore be understood as **a separate work stream.** This is a pre-requisite for an efficient exercise consistent with the mandate of the Directive (EU) 2015/849, especially when the Commission will make recommendations to Member States on the measures suitable for addressing the identified European ML/TF risks. In carrying out the national risk assessments, Member States shall also make use of the findings of the SNRA report.

2. SCOPE AND OBJECTIVE

The aim of this document is to define methodological guidelines, governance, working arrangements and road map in order to support the conduct of the risk assessment and the interactions with relevant stakeholders in terms of inputs, expertise and advice.

[484] O.J. L.141, 5.06.2015, p.73.

The objective and scope of the risk assessment is defined in article 6 of Directive (EU) 2015/849. For the purpose of this methodology, the objective is to carry out an assessment of supranational ML/TF risks.

The "evaluation" of the identified and assessed risks (outcomes of the risk assessment) is out of the scope of these methodological guidelines and shall be considered within the framework of the overall risk management process leading to the identification of mitigation measures to fill the identified residual risks (see **Annex 1**).

3. ROLES AND RESPONSIBILITIES ON EU SUPRANATIONAL RISK ASSESSMENT

3.1. Role of the Commission

Following the mandate given by Article 6 of the Directive (EU) 2015/849, the Commission is responsible for drawing up the SNRA report and for defining the mitigating measures.

The Commission conducts the assessment by:

- organising the work at European level and involving the appropriate experts;

- making the joint opinions of the European Supervisory Authorities (ESAs) as well as the SNRA report available to the Member States and obliged entities;

- defining the mitigating measures, making recommendations to Member States on the measures suitable for addressing the identified risks.

In that context, though the Commission relies on the expertise of several stakeholders (see point 3.3), **it enjoys a decisional power to validate the outcomes of the SNRA discussions.**

An Inter-service Group of the Commission acts as steering group for this exercise

3.2 Role of the ad hoc Working Group

In order to define a risk assessment methodology, an Ad Hoc Working Group (ADHWG) composed by volunteers from Member States was set up in February 2014. The role of the ADHWG was to support the development of the methodology for carrying out the identification, assessment and evaluation of the supranational ML/TF risks as provided for in the Directive (EU) 2015/849. The ADHWG followed the approach defined by FATF in its "Guidance on National Money Laundering and Terrorist Financing Risk Assessment" published on February 2013[485].

3.3 Role of other stakeholders

During each step of the process, the Commission involves the relevant experts from Member States[486] and European bodies as defined in the Directive. Where appropriate, the Commission also involves representatives from the private sector, NGOs or academics in the process. Input and relevant

[485] http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf

[486] Throughout this document, indications about the composition of the Member States experts groups designated to conduct the risk identification and risk assessment are provided for sake of information. However, the appointment of the most relevant experts is left to the appreciation of each Member States by considering the specific expertise required for each dedicated phase of the risk identification and assessment. It may include representatives of supervisory authorities, financial intelligence units, customs, gambling sectors, ministerial authorities, law enforcement, etc.

information could be requested to the following stakeholders through ad hoc processes (public consultation, questionnaires, preparation of background papers, bilateral meetings…):

Experts group on money laundering and terrorist financing (EGMLTF): EGMLTF is a permanent Commission expert group composed of national administrations with the mandate of assisting the Commission, e.g. in the preparation of policy definition and providing expertise to the Commission when preparing implementing measures. EGMLTF has the capacity to draw on expertise available nationally.

- EGMLTF may provide data relating to national risk assessments and more generally information on risks, threats and vulnerabilities. The role of EGMLTF in regard of the SNRA is also to appoint national experts for the different workshops.

European Supervisory Authorities (ESAs): the ESAs (European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority) are tasked under article 6(5) of Directive (EU) 2015/849 with the responsibility of issuing a joint opinion on the ML/TF risks affecting the Union's financial sector.

Considering the key role the ESAs play in the identification of risks related to the financial sector, they participate directly to the discussions held within the ADHWG. In addition, regular contacts are organised between the Commission services responsible to draw up the SNRA report and the working group of the ESAs in charge of the joint opinion.

- ESAs provide data relating to distinctive features of ML/TF risks from a supervisory perspective, ML risks associated with the financial sectors' systems and controls, taking into account the various typical sectorial business models, strategies and cultures..

Other financial supervisory authorities not represented by the ESAs: considering the wide range of actors responsible for financial supervision, contacts will be held with other supervisory authorities not represented in the ESAs.

EU Financial Intelligence Units (EU FIUs): FIUs cooperate at the EU level through a group called the FIU Platform which main task is to facilitate cooperation among EU FIUs. Work of the FIU Platform and the EGMLTF is closely coordinated.

- The FIU Platform provides data relating to national risk assessments, distinctive features of ML/TF risks from an FIU perspective (annual reports), aggregated data on suspicious transactions reports..

Sectorial specific expert groups: the Commission manages a number of groups of Member States experts covering the different sectors exposed to the ML/TF risks. Those networks may provide useful information and data regarding their respective sectors.

- Such experts group are consulted especially for preparing the assessment of the sectors' vulnerability.

Europol: Europol is an EU agency which supports law enforcement authorities by gathering, analysing and disseminating information.

- Europol provides data relating to organised crime threat assessments (e.g. "organised crime threat assessment report" which includes analysis on money laundering threats). It may also provide analyses and intelligence work on AML/CFT from a law enforcement perspective.

Eurostat: Eurostat is a Directorate General of the European Commission which provides statistics at European level that enable comparisons between countries and regions.

- Eurostat provides data relating to series of indicators for the different stages of the AML chain, from the filing of a suspicious transaction report through to conviction. It may also provide statistical data on economy, sectors and products.

Financial Action Task Force (FATF) and FATF-Style Regional Bodies (FSRB): FATF is an inter-governmental body which sets standards and promotes effective implementation of legal, regulatory and operational measures for combating ML, TF and other related threats to the integrity of the international financial system. FSRBs have been established for the purpose of disseminating FATF Recommendations throughout the world. The main task of the FSRBs is to devise systems for combating ML/TF risks in their respective regions.

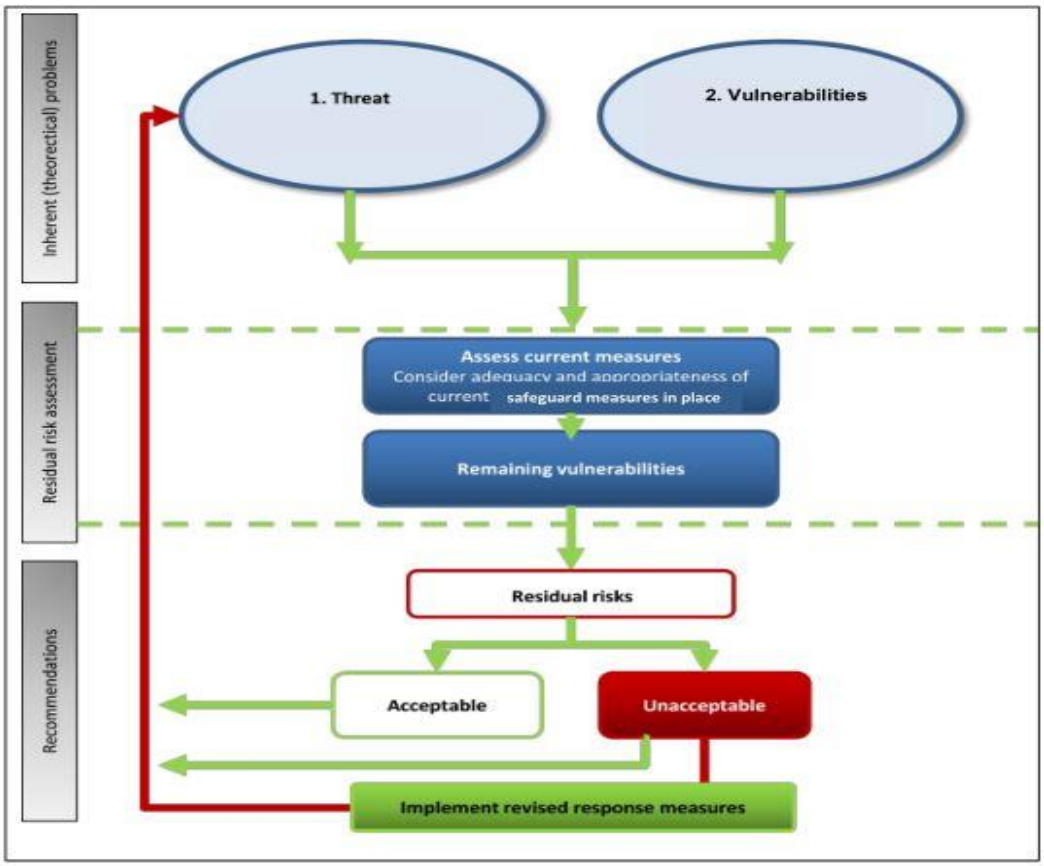
- The FATF and FSRBs conduct evaluations of the AML/CFT systems of the Member States and are developing studies of typologies – the most common schemes used by criminals for ML/TF- that will provide useful information to feed the SNRA.

Other relevant stakeholders such as Non-Governmental Organisations (NGOs), private sector representative bodies at European level (DNBPs, financial sectors etc.) and other public or private sector organisations also provide useful information.

4. METHODOLOGICAL APPROACH

4.1 Risk management framework

The conceptual framework for this methodology can be summarised as follows:



4.1.1 Methodological approach

Because of their specific features, FT and ML risks are considered and assessed within two separate work streams.

The methodology followed is based on the following consecutive actions:

1. **The identification of ML and TF mechanisms** (*modi operandi*) that could constitute ML/TF risks at EU level. There are intended as ML/TF mechanisms going beyond the specificities of national jurisdictions, whatever they arise in one or several Member States and which may represent a risk from an internal market perspective.

2. **An assessment of the level and nature of threats** related to estimated intent and capability to exploit mechanisms for ML and TF, i.e. a clear modi operandi approach by "product/sector" (scenario based approach), at least in all areas mentioned in article 2 and 4 of the Directive (EU) 2015/849. In this specific application, the assessment focuses on the estimated intend and capability of criminals to exploit existing or innovative mechanisms for ML and TF. The assessment is based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available intelligence, information (qualitative and quantitative inputs) and in light of the agreed approach to threat assessment (clearing house threat assessment reconciliation method). The Commission, which has a decisional power to validate the outcomes of the SNRA discussions, assesses the strategic level of threat to be respectively:

    1. Lowly significant (value: 1)

    2. Moderately significant (value: 2)

    3. Significant (value: 3)

    4. Very significant (value: 4)

3. **An assessment of the level and nature of vulnerabilities** by sector to ML/TF exploitable mechanisms (*modi operandi*). The vulnerability assessment focuses on the assessment of existing safeguards in place. Based on Member States' experts and other relevant stakeholders estimates, conducted on the basis of available information (qualitative and quantitative inputs) and in light of the agreed approach to vulnerability assessment (clearing house vulnerability assessment reconciliation method). The Commission, which has a decisional power to validate the outcomes of the SNRA discussions, assesses the strategic level of vulnerability to be respectively:

    1. Lowly significant (value: 1)

    2. Moderately significant (value: 2)

    3. Significant (value: 3)

    4. Very significant (value: 4)

4. **Determination of the residual risk** on the basis of interplay of estimated threats and vulnerabilities for each type of modus operandi. The risk assessment is built on a risk based assessment by product/sector. For each product/sector considered a set of pre-defined *modi operandi* (ML/TF exploitable mechanisms) are assessed in terms of risk as combination of the identified level of threat and vulnerability.

For the purpose of this risk assessment the "impact/consequences" component is regarded as constantly significant and is therefore not assessed. This methodology consequently only looks at the threats and vulnerability components. While it is important to understand the consequences associated with the ML/TF activities (physical, social, environmental, economic and structural consequences), from a methodological point of view it is particularly challenging to measure their consequences in quantifiable or numerical terms. **For the purpose of this risk assessment it is therefore assumed that ML/TF activities generate constant significant negative effects** on the transparency, good governance and the accountability of public and private EU institutions, cause significant damage to EU countries national security and have both direct and indirect impact on the EU economy. From a methodological point of view, as the impact/consequences component is assumed as a fix high value for the specific purpose of this risk assessment, the determination of the residual risk for each scenario (*modus operandi* versus scenario) is the consequence of the combination of the identified level of threat and vulnerability.

5. PROCESS DESCRIPTION

The process can be summarised by the following steps:

5.1. Step 1: Risk Identification

The first step consists in identifying the exact scope in terms of ML/TF risks to be assessed at a later stage of the risk assessment process. For the specific purpose of the SNRA as defined in Directive (EU) 2015/849, risks identification should be intended as defining a list of known or suspected ML/TF threats along with the related sectors exploited by criminals to successfully perpetrate ML and/or TF activities. The risk of ML and TF is not the same in every case. Accordingly, a holistic risk-based approach should be used. While the risks identification process will rely largely on known threats, it is important to give due consideration to innovative or emerging threats for which it is reasonable to assume a lack of consolidated safeguards in place. At this stage, the objective is to identify the nature of the risks scenarios (threats versus exploitable sectors) and those which are the most relevant considering the scope of the risk assessment. It does not seek to assess the level of these risks (significant or non-significant) which will be the objective at a later stage (estimated level of threats and vulnerabilities determining the residual risk).

5.2. Step 2: Threat Component

This second step consists in assessing the level of threat (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the scenario (ML and TF processes versus exploitable sector) identified in step 1[487]. The assessment is based on the estimated combined assessment of **intent and capability** of criminals to change or transfer illegitimate or legitimate funds.

[487] Both the threat and vulnerability assessment are built around a four scale rating. Different rating can be considered but this latter presents the advantage (compared to a three or two scale rating) to capture better qualitative differences between the different risks. The resulting risk level is also based on a four scale rating.

The assessment of the threat level for each identified risk leads to a threat assessment level common to the EU as a whole. At this regard, the strategic level of threat for each risk is assessed according to the threat assessment clearing house reconciliation method.

The Commission validates the outcomes of the threat assessment through the clearing house reconciliation method[488].

The "Intent" component of the threat relies on **known intent** (concrete occurrence of the threat[489]) successful or foiled, and the **perceived attractiveness** of ML/TF through a specific mechanism. While the broad intent to ML/TF is assessed as being constantly high, intent to use specific *modus operandi* differs depending of the attractiveness of the ML/TF modus operandi, and the known existence of AML/CFT safeguards.

The risk assessment therefore considers, on a scenario by scenario basis, the **level of intent** to exploit (IT) ML/TF mechanisms.

The "capability" component of the threat is understood as the capability of criminals to successfully change or transfer the ML proceeds of crime and to successfully transfer illegitimate or legitimate funds to financially maintaining a terrorist network.

The assessment of the capability component considers the ease of using a specific ML/TF modus operandi for (technical expertise and support required), the accessibility and relative costs (financial capacity) of using a specific modus operandi.

5.3. Step 3: Vulnerability

This third step consists in assessing the level of vulnerability (lowly significant (1), moderately significant (2), significant (3), very significant (4)) for each of the scenario (ML and TF processes versus exploitable sector) identified in step 1.

For each of the scenario identified in step 1, the vulnerability assessment focuses on the existence and effectiveness of safeguards in place. The more effective safeguards in place, the lower vulnerabilities and risk are.

The vulnerability assessment is performed for the products/sectors, related to the *modus operandi* identified in step 1, required to implement the AML/CFT legislation.

For the specific purpose and scope of the SNRA, the vulnerability assessment considers primarily the existence of national, EU and international legislation and their effective implementation at national level. By taking into account the EU wide nature of the ML/TF risks to be considered in the SNRA, particular attention is paid to other criteria such as the effectiveness of information sharing among FIU, coordination with other AML authorities and international cooperation, including between AML supervisors.

The assessment of ML/TF vulnerabilities of the system as a whole is based on the data collected and analysed by relevant supervisory authorities, the FIU and national authorities.

[488] The clearing house reconciliation method has proven its efficacy in the framework of several EU risk assessments in the field of aviation security. For those risk assessments requiring a common EU position, which is the case for the supranational FT/ML risk assessment, the clearing house reconciliation method has proved its efficacy in providing the necessary working arrangements facilitating the achievement of a common position.

[489] It measures the concrete occurrence of the threat on the territory. The data used originate from the evidence available on the subject of reports to the particular offence or class of offences.

5.4. Step 4: Residual Risk

The outcomes of steps 2A/B (threat assessment) and 3A/B (vulnerability assessment) determine the risk level for each identified risk (steps 1A/B), as combination (matrix approach) of the assessed threat and vulnerability level.

Threat					
	Very significant				
	Significant				
	Moderately significant				
	Lowly significant				
		Lowly significant	Moderately significant	Significant	Very significant
		Vulnerability			

The risk level is ultimately determined by combination between the threat versus vulnerability. The risk matrix determining this risk level is based on a weighting of 40% (threat) + 60% (vulnerability) – assuming that the vulnerability component has more capacity in determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given *modus operandi* – thus impacting ultimately the level of threat.

Threat					
	Very significant	2,2	2,8	3,4	4
	Significant	1,8	2,4	3	3,6
	Moderately significant	1,4	2	2,6	3,2
	Lowly significant	1	1,6	2,2	2,8
		Lowly significant	Moderately significant	Significant	Very significant
		Vulnerability			

RISK	
1 – 1,5	Lowly significant LOW
1,6 – 2,5	Moderately significant MEDIUM
2,6 – 3,5	Significant HIGH
3,6 – 4	Very significant VERY HIGH

6. INVOLVEMENT OF PRIVATE SECTOR AND CIVIL SOCIETY

The Commission has consulted the private sector and civil society during the process as discussed in point 2 ("Methodology followed…") of the SWD.

7. REASSESSMENT

Under the current rules (Article 6 ("Risk Assessment") of the Anti-Money Laundering Directive), based on available intelligence and information, the Commission proposes further rounds of the risk assessment to reassess the evolving threat situation or new emerging threats and ensures an updating of the risk assessment every two years, or more frequently if appropriate.

The first update of the SNRA took place in 2019, 2 years after the issuing of the initial SNRA report. This first update was drawn up through the so-called 'lighter procedure'. It focused on the implementation of the Commission recommendations concerning the mitigating measures, and the evaluation of the risks following the mitigation. It also included new emerging risks, not previously treated.

This second update (initially due by 2021, but delayed by the effects of the COVID-19 pandemic) builds upon the previous assessment outcomes, updating and fine-tuning their conclusions and following, where necessary, brand new analysis of the sectors involved (f.i.: gambling sectors, e-money, crypto-currencies) and re-calculation of the risks presented.

7.1. The European Court of Auditors (ECA)'s special report

In June 2021 the ECA presented its special report 13/2021[490] pursuant to Article 287(4), second subparagraph, TFEU. The report acknowledges the existence of a certain degree of fragmentation at institutional level and finds poor coordination at EU-level when it comes to actions aimed at preventing money laundering and terrorist financing.

As regards the Commission's assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, the audit indicates that

> *the risk assessment carried out by the Commission (Supra-national risk assessment, SNRA) lacks a geographical focus, and does not prioritise risk effectively;*

In its **Recommendation 1**, the ECA indicates that the Commission should improve its risk assessments by

> (using) *greater prioritisation of sectors based on risk throughout the whole supra-national risk assessment exercise: from planning to follow-up, specifying when and why they are changing; and carrying out updates for fast-moving sectors and adding a geographical dimension, where relevant;*

The Commission has worked on addressing recommendation 1 on improving risk assessments starting with the current exercise. A geographical dimension is added, where relevant and possible, to the assessments conducted.

[490] ECA's Special Report 13/2021: EU efforts to fight money laundering in the banking sector are fragmented and implementation is insufficient, https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=58815

The audit report also highlights that the forthcoming legislative reform is an opportunity for the Commission, the European Parliament and the Council to address the weaknesses identified and to remedy the fragmentation of the EU AML/CFT framework.

7.2. SNRA in the 2021 legislative proposal

Specifically as regards the Commission's SNRA, this proposal, as it builds on Directive (EU) 2015/849, is consistent with the recommendations of the Financial Action Task Force (FATF) and the frequency of the supra-national risk assessment is also brought in line with best practices recognised and indicates it will take place every 4 years.

The proposal also integrates the changes brought about by the recent revisions of the FATF recommendations in relation to assessment and mitigation of risks of evasion of targeted financial sanctions.

More in detail, its is proposed that the assessment will be based on input from the Anti-Money Laundering Authority (AMLA) in the form of an Opinion, and be accompanied by recommendations to Member States on the measures suitable for addressing the identified risks. The Commission will also report every four years to the European Parliament and the Council on the actions taken in reaction to the findings of the assessment. It is also proposed that the Commission may update parts of the report more frequently, if appropriate.

National risk assessments will continue to be carried out by Member States but with a minimum frequency of every four years, and with certain additions to the objectives and modalities of such assessments. Member States must also continue to maintain comprehensive statistics on AML/CFT and transmit them to the Commission annually. The Commission may adopt an Implementing Act on the methodology for such statistics.

ANNEX III

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 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 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.
- Directive 2014/65/EU on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
- 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.
- Delegated Regulation (EU) 2016/1675 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council.
- Regulation (EU) 2019/2175 of the European Parliament and of the Council of 18 December 2019 amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds.

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:

- Regulation (EU) 2018/1672 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005.

Additional preventative measures:

- Regulation (EU) 2019/880 on the introduction and the import of cultural goods.

Other EU laws that interact with the AML Directive:

- Directive 2014/92/EU, the Payment Accounts Directive.
- Directive 2014/49/EU, the Deposit Guarantee Schemes Directive.
- Regulation (EU) 2015/847, the Wire Transfer Regulation.

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 the ISIL (Da'esh) and Al-Qaida organisations.
- Council Regulation (EU) No 753/2011 of 1 August 2011 concerning restrictive measures directed against certain individuals, groups, undertakings and entities in view of the situation in 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 Framework Decision 2001/500/JHA on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime.
- 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.
- 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.
- 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.
- Directive (EU) 2018/1673 on combating money laundering by criminal law.
- Directive (EU) 2019/1153, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.

Legal acts relating to Europol's competence to offer support in preventing and combating money laundering and financing of terrorism (support to FIUs and LEAs), notably:

- Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol)
- Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation

ANNEX IV

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
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/
Europol	The European Union Agency for Law Enforcement Cooperation
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
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
NFT	Non-fungible tokens
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 Centre
PEP	Politically Exposed Person
PIC	Private Investment Company
PSD	Payment Services Directive
RBA	Risk Based Approach
ROE	Report of Examination
SAR	Suspicious Activity Report
SCI	Société Civile Immobilière
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 Reports

ANNEX V

BIBLIOGRAPHY

1. Commission documents

- Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing 2020/C 164/06, C/2020/2800, *OJ C 164, 13.5.2020, p. 21–33.*
- Communication from the Commission on the EU Security Union Strategy, COM/2020/605 final.
- Commission Staff Working Document on the movement of capital and freedom of payments, SWD(2020) 39 final.
- *Commission's package of legislative proposals to strengthen the EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules:* https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en

2. European Parliament documents

- Anti-money-laundering package. Briefing - Initial Appraisal of a European Commission Impact Assessment: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)699467
- Procedure file: 2021/0250(COD), Prevention of the use of the financial system for the purposes of money laundering or terrorist financing: mechanisms to be put in place by the Member States: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0250(COD)&l=en
- Procedure file: 2021/0240(COD), Anti-Money Laundering Authority (AMLA): https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0240(COD)&l=en

3. 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
- The European Union (EU) Serious and Organised Crime Threat Assessment (SOCTA) (2021): https://www.europol.europa.eu/publications-events/main-reports/socta-report
- Europol's annual EU Terrorism Situation and Trend Report (TE-SAT) (2022) https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf
- EFIPPP typology reports

4. Other EU-level bodies

- ECB Payments statistics 2020: https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2020~5d0ea9dfa5.en.html
- Opinion of the European Banking Authority on communications to supervised entities regarding money laundering and terrorist financing risks in prudential supervision: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/a8270e12-b0c2-4194-a70f-1f1ece5c71a3/Opinion%20on%20Communication%20of%20ML%20TF%20risks%20to%20supervised%20entities.pdf?retry=1
- Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector:

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

- EBA's Guidelines on risk-based supervision (revised): https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism/guidelines-risk-based-supervision-revised

5. FATF and Moneyval reports

- Moneyval Annual Report: https://rm.coe.int/annual-report-2020-eng-final/1680a429f5
- FATF focus on COVID-19: https://www.fatf-gafi.org/publications/covid-19/covid-19.html?hf=10&b=0&s=desc(fatf_releasedate)
- FATF focus on virtual assets: https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)
- FATF focus on terrorist financing: https://www.fatf-gafi.org/publications/fatfgeneral/documents/terroristfinancing.html

6. Other external information sources

- Anti-Money Laundering in the EU – CEPS: https://www.ceps.eu/ceps-task-forces/anti-money-laundering-in-the-eu/
- Mapping the risk of serious and organised crime infiltration in Europe – Final Report of the MORE project: https://www.transcrime.it/wp-content/uploads/2018/12/MORE_FinalReport.pdf
- "La economía ilícita en España", Fernández Steinko, A.; Alianza Ensayo, 2021. Mapping Project: https://www.ucm.es/afsteinko/tablas-y-apuntes-metodologicos
- Transcrime: https://www.transcrime.it/en/
- Anti-Money Laundering Europe (AME): https://www.amleurope.com/
- FinCEN files: https://www.icij.org/investigations/fincen-files/
- Transparency International EU - Anti-money laundering: https://transparency.eu/priority/financial-flows-crime/anti-money-laundering/

7. Confidential information

Information was received from Europol and several FIUs (classified).

8. Written contributions from the following stakeholders

From 2020 to 2022 the Commission has maintained close contacts with the following private-sector stakeholders, representatives of financial institutions, 'designated non-financial businesses and professions' (DNFBPs), representatives of the civil society (NPOs). National associations were represented through their respective European federation:

- Accountancy Europe

- Aforeconsulting
- Antwerp World Diamond Centre (AWDC)
- Assuralia
- ATG
- City of Amsterdam - EUROPEAN FORUM for URBAN SECURITY
- Civil Society Europe
- The Council of Bars and Law Societies of Europe (CCBE)
- DAFNE
- ECNL
- Edenred
- Electronic Money Association (EMA)
- European Association of Real Estate Professions (CEPI)
- European Federation of Jewellery (EFJ)
- European Foundations Centre
- European Fundraising Association (EFA)
- European Payment Institutions Federation (EPIF)
- Eurofinas
- European Association of Cooperative Banks (EACB)
- European Association of Public Banks (EAPB)
- European Casino Association (ECA)
- The European Gaming and Amusement Federation (EUROMAT)
- European Gaming & Betting Association (EGBA)
- European Lotteries
- Insurance Europe
- Joint Research Centre on Transnational Crime (TRANSCRIME)
- King Baudouin Foundation
- Moneygram
- NGO Voice
- Notaires d'Europe
- Notariado ES
- Pari Mutuel Urbain
- Paypal
- RIA Money Transfer
- Schuman Associates
- Sport Integrity Global Alliance (SIGA)
- Taxadvisers Europe
- Transparency International EU
- TRUSTEUAFFAIRS
- UEFA (Legal Committee)
- Università Catolica del Sacro Cuore
- VENRO
- Western Union

The Commission has also contacted and greatly benefitted from the input of national designated experts (especially in the 'virtual assets and related services area') and academics working specifically in AML/CTF-mapping projects. The Commission would like to thank them all for their collaboration and disinterested support during this exercise.