EUROPEAN
COMMISSION

Brussels, 26.6.2017
COM(2017) 340 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

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

{SWD(2017) 241 final}

1. INTRODUCTION

Money laundering and terrorism financing are significant and evolving challenges which need to be addressed at European Union (EU) level. The recent terrorist attacks and recurring financial scandals call for stronger action in this area.

In the context of the internal market, financial flows are integrated and cross-border by nature, and money can flow swiftly, if not instantly, from one Member State to another, allowing criminals and terrorists to move funds across countries avoiding detection by authorities.

To address these cross-border phenomena, the EU Anti-Money Laundering/Counter-Terrorism Financing (AML/CFT) framework has defined common rules on the controls and reporting obligations by financial institutions and other economic actors and established a robust framework for EU Financial Intelligence Units (FIUs) to analyse suspicious transactions and cooperate among each other. Despite substantial and steady progress in this area, renewed efforts and additional measures to close any potential gaps are still needed to effectively combat money laundering (ML) and terrorist financing (TF).

This report on the supra-national risk assessment (SNRA) of the risks of ML and TF affecting the internal market and relating to cross-border activities is the first report carried out at a supranational level in the EU. It analyses the risks of ML and TF the EU could face and proposes a comprehensive approach to address them.

Under Article 6 of Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of the ML or TF (the Fourth Anti-Money Laundering Directive, or 4AMLD)[1] requiring the Commission must draw up, by 26 June 2017, a report identifying, analysing and evaluating the ML and TF risks at Union level. The publication of this SNRA is also one of the deliverables of the European Security Agenda[2], and the Action Plan on Terrorist Financing[3].

Having a clear understanding and analysis of ML and TF risks is a pre-requisite before any efficient and adequate policy response can be made. Risk assessment is particularly important for the internal market given that financial flows are integrated and cross-border by nature.

The SNRA uses a defined methodology[4] to provide a systematic analysis of the ML or TF risks linked to the modi operandi used by perpetrators. The aim is not to pass judgment on a sector as a whole, but to identify circumstances in which the services and products it delivers or provides could be abused for TF or ML purposes. This SNRA is based on Directive 2005/60/EC (3AMLD), the legislation in force at the time of the analysis. It describes the areas in which, at the time, the EU legal framework was not as harmonised or complete as it would be once the subsequent revisions of 3AMLD had taken effect.

[1] The deadline for transposing this Directive into national laws is 26 June 2017
[2] COM(2015) 185 final, 28.04.2015
[3] COM(2016) 50 final, 02.02.2016
[4] For a more detailed description of the methodology, see the Staff Working Document (2017) 241

This SNRA focuses on vulnerabilities identified at EU level, both in terms of legal framework and in terms of effective application. It does not prejudge the mitigating measures that some Member States are applying or may decide to apply in response to their own national ML/CFT risks. They may therefore be implementing some of the recommendations below already, or have adopted stricter rules than the minimum rules defined at EU level. The assessment of vulnerabilities mitigating measures identified in this report should therefore be considered a baseline that could be adapted, depending on the national measures already in place.

Under Article 6 of 4AMLD, in the event that Member States that decide not to apply any of the suggested recommendations in their national anti-money laundering and counter-terrorism financing (AML/CFT) regimes they should notify the Commission of their decision and provide a justification for it ("comply or explain").

This report presents the main risks for the internal market in a wide range of sectors and the horizontal vulnerabilities which can affect such sectors. On this basis, this report presents the mitigating measures that should be pursued at EU and national level to address these risks and puts forward a number of recommendations for the different actors involved in the fight against ML and TF.

While the Commission acknowledges the risks posed by some high-risk third countries, such geographical risk analysis was not part of this first SNRA. This is due to the fact that the analysis of the risks posed by these jurisdictions is currently conducted in the context of a separate process, namely the Commission delegated acts identifying third-country jurisdictions which have strategic deficiencies that pose significant threats to the EU financial system for ML/TF.[5].

2. OUTCOMES OF THE SNRA

The Commission has identified 40 products or services that are considered potentially vulnerable to ML/TF risks affecting the internal market. These cover 11 professional sectors, including all those defined by the 4AMLD, along with some not included in the scope of the Directive but considered relevant for the SNRA[6]. This has enabled the Commission to pinpoint the areas of the internal market that are at greatest risk and represent the most widespread means used by criminals. The SNRA focuses first and foremost on the risks associated with each relevant sector. At the same time, in assessing the measures recommended to address such risks, the Commission has looked at the most widespread means used by criminals.

2.1. Main risks to the internal market in the sectors covered by the SNRA[7]

[5] Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies. In addition, an EU listing process is ongoing in order to identify and address third countries that fail to comply with tax good governance standards (COM(2016) 24 final).

[6] These risks are linked to the use of cash, virtual currencies, crowdfunding, non-life insurance and non-profit organisations, as well as Hawala and other similar informal value transfer services' providers.

[7] The accompanying staff working paper contains a detailed analysis of the level of threat and vulnerability to ML and TF faced by each sector when delivering specific products or services.

2.1.1. Financial sector

The financial sector has been covered by the EU AML/CFT framework since 1991 and seems to have a good awareness of its risks. While terrorists and criminals are still trying to use the financial sector for their activities, the assessment shows that the level of ML/TF risks to the financial sector is moderately significant due to the mitigating measures already in place.

However, the risk of money laundering remains significant for certain segments in the financial sector, such as **private banking and institutional investment** (especially through brokers). This is due to the overall higher exposure to product and customer risks, pressures of competition in the sector and a limited understanding among supervisors of their operational AML/CFT risks. **Safe custody services** are also seen as significantly exposed to ML risks due to limitations in monitoring capacities for obliged entities – and the existence of non-regulated storage facilities (e.g. free zones).

Electronic money or money value transfer services (i.e. money remittances)[8] are considered as significantly and even highly significantly exposed to ML/TF risks - the first sector because of their anonymity features under 3AMLD and the second because of uneven monitoring capacities among obliged entities. For **currency exchange offices and money remittances**, applying AML/CFT rules to occasional transactions only above EUR 15 000 seems problematic since criminals can make smaller transfers over time. This is especially problematic in the absence of a common definition of operations which are linked or have an actual element of duration.

Emerging products – such as **crowdfunding platforms and virtual currencies** – appear to be significantly exposed to ML/TF risks. Some Member States have decided to address these financial products in national law, but overall the EU legal framework under 3AMLD remains inadequate. **FinTech**[9] aims to introduce new technological solutions for speedier, securer and more efficient financial products but also could open up opportunities for criminals. In order to adapt to ongoing technological developments, further analysis will be required to understand what risks products in this fast-developing sector may pose and to leverage the possibilities of new technologies to improve AML/CFT efforts.

Finally, the assessment has shown that fraudulent application of **consumer's credit and low value loans** has been a recurrent practice in recent terrorist cases. There is a low level of awareness and diverging application of AML/CFT requirements at national level for such products.

2.1.2. Gambling sector

Under 3AMLD, the gambling sector has not been subject to AML/CFT requirements except for casinos. Under 4AMLD all providers of gambling services become obliged entities. However Member States may decide to grant full or partial exemptions to

---

8 Article 4(22) of Directive (EU) 2015/2366 defines 'money remittances' as a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

9 'FinTech' refers to technology-enabled and technology-supported financial services. Technology has the potential to facilitate access to financial services and to make the financial system more efficient 'Reg Tech' is about adopting new technologies to facilitate the delivery of regulatory requirements.

providers of certain gambling services, on the basis of a proven low risk. Member States should take into consideration the relevant findings of this SNRA.

At this stage, certain gambling products are considered as significantly exposed to ML risks. In the case of **land-based betting** and **poker**, this seems to be particularly due to inefficient controls. This is either because, by their nature, these activities involve significant volumes of speedy and anonymous transactions often cash based or a peer-to-peer element with a lack of proper supervision. When **gambling online**, there is high-risk exposure due to the huge volumes of transactions/financial flows and non-face-to-face element. Online gambling allows for anonymous means of payments, but at the same time offers an important mitigating feature in the form of transaction-tracking. **Lotteries and gaming machines** (outside casinos) present a moderate level of ML/TF risks. Lotteries have developed a certain level of controls, in particular to address risks associated with high winnings. Although **casinos** present inherently high-risk exposure, their inclusion in the AML/CFT framework since 2005 has had a mitigating effect on ML/CFT risks. **Land-based bingo** is seen as presenting a low level of ML/TF risks due to its relatively low stakes and winnings.

2.1.3. Designated non-financial businesses and professions

Overall, the non-financial sector's exposure to ML/TF risks is considered as significant and even highly significant. The identification of the **beneficial owner** of the customer seems to be the main weakness in this sector, especially for **trust and company services providers, tax advisors, auditors, external accountants, notaries and other independent legal professionals**. The analysis has shown that sometimes the concept of beneficial owner itself is either not properly understood or not correctly checked when entering into a business relationship.

In the specific case of professionals carrying out activities covered by the legal privilege principle (tax advisors, auditors, external accountants, , notaries and other independent legal professionals), the implementation of AML/CFT rules appears challenging. Legal privilege is an important, recognised principle at EU level. It reflects the delicate balance stemming from the European Court of Justice case-law on the right to a fair trial[10], itself reflecting the principles of the European Court of Human Rights and the Charter of Fundamental Rights of the European Union (such as article 47).

Under the EU AML framework[11], such professionals are exempted from reporting obligations when defending a client in a judicial proceeding (legal privilege) which increases the risk of misuse. In effect, there are cases where these professionals sometimes conduct activities that are clearly covered by the very essence of the legal privilege (i.e. ascertaining the legal position of their client or defending or representing their client in judicial proceedings) alongside activities not covered by it, such as providing legal advice in the context of the creation, operation or management of companies. It appears that there are situations where some such professionals might consider all these activities as captured by the legal privilege principle. This might result in a failure to comply with AML/CFT obligations for part of the activities. It is important to stress that compliance with AML/CFT rules does not interfere in any way with the principle of legal privilege. At the same time, its **interpretation and application** by professionals carrying out activities covered by the legal privilege principle could be improved. A better understanding by tax advisors, auditors, external accountants, ,

[10] See case C-305/05
[11] See Article 23(2) of Directive 2005/60/EC

notaries and other independent legal professionals would also be beneficial, as they are also considered obliged entities under the 4AMLD.

In addition, based on the current EU legal framework, self-regulatory bodies are designated to supervise tax advisors, auditors, external accountants, , notaries and other independent legal professionals and estate agents[12]. Member States are free to decide that these self-regulatory bodies are competent to receive the suspicious transactions reports (STRs) directly from the obliged entities, being then responsible for sending them to the Financial Intelligence Unit (FIU) promptly and unfiltered. The consultations have shown that obliged entities and self-regulatory bodies in this sector do not report many suspicious transactions to the FIUs especially in certain Member States. This could be an indication either that the suspicious transactions are not correctly detected and reported, or that the self-regulatory body does not ensure a systematic transmission of the suspicious transactions reports (STR).

The **real estate sector** is also exposed to significant ML risks, due to the variety of professionals involved in real estate transactions (real estate agents, credit institutions, notaries and lawyers). Another common means of laundering proceeds is over-invoicing in commercial trade '**trade-based money laundering**') or setting up fictitious loans. Perpetrators use such methods as a means to justify moving criminal proceeds through banking channels, often using false documents to trade in goods and services. Similarly, fictitious loans are often set up between them in order to create a fictitious financial transaction in view of justifying transfers of funds of illegal origin. Such risk is considered as significant by law enforcement authorities.

2.1.4. Cash and cash-like assets [13]

The SNRA has shown that **cash** remains the most recurring means used for ML/TF purposes, since it allows criminals to conceal their identity. That is why it appears in almost every AML/CFT investigation. Under 3AMLD, cash transactions have not been properly monitored in the internal market because of a lack of clear regulation and controls requirements. Some Member States have introduced cash transactions reports (CTR) or limits on cash payments. But in the absence of common requirements for all Member States, criminals may easily exploit differences in legislation. Similarly, the EU framework for controls on cash couriers at the EU external border[14] does not ensure adequate levels of mitigation, especially since it does not cover cash-like products such as highly liquid commodities including gold, diamonds or high-storage anonymous prepaid cards.

In addition, the risks posed by **dealers in high-value goods** accepting cash payments in cash over EUR15 000 are considered significant because of the inherent risk exposure and the weak level of controls. The fact that such traders are subject to AML/CFT rules only to the extent that they accept high-value cash payments seems to lead to ineffectiveness in applying those rules. The challenge is even more important with regard to **cash-intensive businesses**. These are not subject to AML/CFT rules, unless they fall

[12] Directive 2015/849 (EU) defines self-regulatory body as a body that represents members of a profession or has a role in regulating them, in performing certain supervisory or monitoring type functions and in ensuring the enforcement of the rules relating to them.

[13] Multipropose cash transfers in humanitarian aid operations funded by the EU are not concerned

[14] Regulation (EC) No 1889/2005 of 26 October 2005 on controls of cash entering or leaving the Community

into the above-mentioned category of dealers in high-value goods. But they may very conveniently serve for laundering cash-based proceeds from criminal activities.

The assessment also stresses that assets offering similar facilities to cash (**gold, diamonds**) or high-value, easily tradable "lifestyle" goods, (e.g. **cultural artefacts, cars, jewellery, watches**) are also high-risk, because of weak controls. Specific concerns have been expressed about looting and trafficking of antiquities and other artefacts: looted artefacts could serve as a source of terrorist financing – or alternatively artefacts are attractive as placement for money laundering.

2.1.5. Non-profit organisations

Non-profit organisations (NPOs) may be exposed to the risks of being misused for TF purposes. The analysis of the NPO's sector vulnerability to TF has been rather challenging as this sector is characterised by a variety of structures and activities which present varying degrees of risk exposure and risk awareness. This is mostly due to the diverging NPO landscape and differences in legal frameworks and national practices. "Expressive NPOs"[15] present some vulnerability because they may be infiltrated by criminal or terrorist organisations that can hide the beneficial ownership making the traceability of the collect of funds less easy, while some types of "Service NPOs'"[16] are more directly vulnerable due to the intrinsic nature of their activity. This is due to the fact they may involve funding to and from conflict areas or third countries identified by the Commission as presenting strategic deficiencies in their AML CFT regimes[17]. Nevertheless, it has been considered during the analysis that this variety in the NPOs landscape does not prevent the identification of common characteristics of the NPOs sector's vulnerabilities.

In that context, the analysis has shown that the existing AML/ CFT requirements are not necessarily considered by the competent authorities as adequate to address the specific needs of the NPO sector and controls in place differ, depending on the Member State concerned. It is acknowledged that controls in place are more efficient when dealing with collection of funds within the EU which makes the level of vulnerabilities lower than for transfers of funds or expenditure outside the EU where more material weaknesses remain.

More generally, the assessment of the NPO sector has revealed that it may undergo de-risking i.e. some financial institutions may be reluctant to provide it with financial services such as opening a bank account. Some financial transactions may be refused, depending on the country of destination of the funds. In addition, smaller organisations not able to demonstrate that they hold accreditation or tax proof of registration may find themselves unable to open bank accounts. According to NPO representatives, exclusion from the provision of financial services increases the use of cash, which is much more vulnerable to ML/TF abuses.

---

[15] "Expressive NPOs" are NPOs predominantly involved in expressive activities, which include programmes focused on sports and recreation, arts and culture, interest representation, and advocacy

[16] "Services NPOs" are NPOs involved in diverse activities, such as programmes focused on providing housing, social services, education, or health care.

[17] Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies

The issue of de-risking or financial exclusion is a concern that should be kept in mind when addressing AML/CFT policy. Customers must not be rejected by regulated financial providers and compelled to use underground banking or underground transfer services. However, AML/CFT is only one of the many drivers of de-risking. At EU level, the adoption of the 'Payments Account Directive[18]will greatly boost access to basic financial services that would likely limit the reliance on informal channels.

2.1.6. Hawala

While value transfer services present their own risks, Hawala[19] and other such informal value transfer services pose a specific threat, particularly in the context of TF. Normally, all operators providing payment services as defined in Article 4(3) of Payment Services Directive 2 (PSD2)[20] should be appropriately registered and regulated. Those providers should seek the status of authorised payment institutions or, under certain conditions, registered payment institution. Hawala and other such informal value transfer services usually qualify as illegal since they are usually not registered and do not comply with the requirements of PSD2. This problem is compounded by the difficulty in detecting the existence of Hawala or other such services: the transactions are often bundled, compensated via goods imports/exports, and leave limited information trail. De-risking is also relevant in this respect, as customers rejected by regulated financial service providers, sometimes resort to illegal services of this kind.

2.1.7. Currency counterfeiting

Currency counterfeiting is a transnational type of illegal activity with a high level of cross-border movements of both criminals and counterfeit currency, and it often involves organised crime groups. The smuggling of counterfeit currency generates proceeds of crime which need to be laundered for their integration into the regular financial stream. In addition currency counterfeiting could be distributed through terrorist networks to fund training, recruitment, attacks and propaganda, which requires large amounts of funds. Proceeds of counterfeiting could be invested to strengthen terrorist support infrastructure.

2.2. Horizontal vulnerabilities

The Commission has identified a number of vulnerabilities common to all sectors.

2.2.1. Anonymity in financial transactions (cash and other anonymous financial products)

Criminal organisations or terrorist groups try to avoid leaving any information trail and to remain undetected when committing illegal activities. By their very nature, cash transactions allow for complete anonymity, making them very attractive payments/transfers methods for perpetrators. Sectors exposed to a high level of cash

[18] Directive 2014/92/EU of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

[19] Hawalas and other similar service providers (HOSSPs) arrange for the transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. What makes them distinct from other money transmitters is their use of non-banking settlement methods.

[20] Directive (EU) 2015/2366 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.

transactions are considered particularly at risk. This is especially relevant for cash-intensive businesses, traders in goods and services accepting payments in cash, and economic operators accepting payments in large value denominations, such as EUR 500 and EUR 200 banknotes.

Financial products offering similar anonymity features in certain circumstances (such as anonymous electronic money products, virtual currencies or crowdfunding platforms) are also vulnerable to ML and TF. Their risk levels differ compared to cash transactions because they require more sophisticated planning, cover lower volumes of transactions and may be subject to a certain level of monitoring. However, their anonymity features place an intrinsic limitation on identification and monitoring possibilities. The same analysis applies to other types of assets such as gold and diamonds that are easily tradable or can be safely stored. These are easy to transfer and allow for anonymity at the same time.

2.2.2. Identification and access to beneficial ownership information

Criminals also use the financial system to put their illicit proceeds into financial markets, real estate or the legitimate economy in a more structured way than with cash or anonymous financial transactions. Firstly, all sectors are vulnerable to risk of infiltration, integration or ownership by organised crime organisations and terrorist groups. Secondly, a common technique for criminals is to create shell companies, trusts or complicated corporate structures to hide their identities. In such cases, while the funds involved may be clearly identified, the beneficial owner remains unknown. According to law enforcement authorities' information, in major ML/TF cases opaque structures have been recurrently used to hide the beneficial owners. This widespread issue is not limited to certain jurisdictions or certain types of legal entities or legal arrangements. Perpetrators use the most convenient, easiest and securest vehicle depending on their expertise, location, and the market practices in their jurisdiction.

3AMLD contains rules on defining beneficial ownership when entering into a business relationship. The 25% share ownership threshold for defining a controlling element is only indicative and identifying the 'senior manager' as beneficial owner is only a last resort when no other beneficial owner can be identified after a documented in-depth assessment (e.g. split shareholdings). However, in practice the rules may be applied mechanically by certain obliged entities. In such circumstances, it is questionable whether this leads to the identification of the real beneficial owner.

2.2.3. Supervision within the EU internal market

Certain vulnerabilities with the effectiveness of financial supervision in a cross-border context are apparent. According to the joint opinion of the European Supervisory Authorities (ESAs)[21], competent authorities' assessment of the compliance of the sector they supervise varies significantly. The most challenging aspect concerns situations where entities that belong to the same financial group are subject to the supervision of competent authorities from several Member States. These situations make implementing AML/CFT rules rather complex because of lingering differences between competent authorities in their approach to AML/CFT supervision and because of uncertainty about home/host supervisory responsibilities in particular for payment institutions and their

[21]http://www.eba.europa.eu/documents/10180/1759750/ESAS+Joint+Opinion+on+the+risks+of+money+laundering+and+terrorist+financing+affecting+the+Union%E2%80%99s+financial+sector+%28JC-2017-07%29.pdf

foreign agents. This creates a risk that breaches or cases of abuse for financial crime purposes will go undetected. In addition, it seems that the relevant information is sometimes not shared sufficiently or in a good time amongst the competent AML/CFT supervisors.

There are several reasons for this:
- differences in the counterparts' status;
- an inadequate framework to exchange confidential AML/CFT information;
- an excessive focus on pure prudential supervision; and
- a lack of legal framework/mechanisms for information exchange between prudential supervisors and AML/CFT financial supervisors[22].

Lastly, in some limited cases, supervisors have difficulty in identifying the relevant counterparts since in some Member States AML/CFT supervision is fragmented. The joint opinion also mentions that some supervisors do not adequately identify the AML/CFT risks linked to the sectors they supervise, and/or do not have sufficient or dedicated risk-based procedures in place to supervise these risks, especially in the TF area.

As regards non-financial sectors, Member States may allow the self-regulatory bodies to perform supervisory functions for tax advisors, auditors, external accountants, , notaries and other independent legal professionals and estate agents. Whatever the supervisory model followed, the supervision suffers from weaknesses in terms of controls, guidance and level of reporting in the large majority of Member States.

2.2.4. Cooperation between FIUs

The FIUs are responsible for receiving and analysing information on suspicious financial activities relevant to ML, TF and associated predicate offences, and for disseminating the results of their analysis to the competent authorities. This analysis is crucial for law enforcement authorities to start new investigations or complement existing ones. Although the collaboration between EU FIUs has increased significantly over the last decade, certain vulnerabilities in FIUs cooperation still remain.

An FIU platform[23]mapping report has extensively identified obstacles to accessing, exchanging and using information and to operational cooperation between FIUs. The mapping report was concluded in December 2016[24]. It also highlights core legal, practical and operational issues. Based on this, and its own analysis, the Commission has outlined possible avenues to improve cooperation of EU FIUs in a separate Staff Working Document[25].

2.2.5. Other vulnerabilities common to all sectors

The SNRA has shown that all the identified sectors are exposed to some additional vulnerabilities:

---

[22] For instance, currently the ECB cannot provide national AML/CFT supervisors with confidential prudential information that is also relevant for AML/CFT supervision.

[23] The FIU Platform is an informal group, set up by the Commission in 2006, which brings together EU Member States' Financial Intelligence Units.

[24] EU Financial Intelligence Units' Platform (reference E03251) http://ec.europa.eu/transparency/regexpert/

[25] SWD (2017)/275

- **infiltration by criminals**: criminals sometimes may become owners of an obliged entity or look for obliged entities willing to assist them in their ML activities. This makes fit-and-proper tests relevant for all analysed sectors;
- **forged documents**: modern technology is making easier to create forged documents and all sectors are struggling to put in place robust mechanisms to detect them;
- **insufficient information-sharing between the public and the private sector**: all obliged entities have stressed the need for proper feedback mechanisms from FIUs and information-sharing with competent authorities. The reporting of suspicious transactions by obliged entities operating across national jurisdictions is another apparent difficulty;
- **insufficient resources, risk-awareness and know-how to implement AML/CFT rules**: whereas certain obliged entities invest in sophisticated compliance tools, many of them have more limited awareness, tools and capacities in this field; and
- **new risks emerging from FinTech**: the use of online services is expected to increase further in the digital economy, boosting demand for online identification while presenting an augmented risk from those non-face-to-face transactions. The use and reliability of electronic identification is crucial in this respect.

3. MITIGATING MEASURES TO ADDRESS THE IDENTIFIED RISKS

Having assessed risk levels, this report outlines the measures that the Commission considers should be pursued at EU and Member State level. They stem from an assessment of possible options to address the identified risks. During this balancing exercise, the Commission took into account:
- the level of ML/TF risks;
- the need and proportionality involved in taking action or recommending that Member States take action;
- the need and proportionality involved in recommending regulatory or non-regulatory measures; and
- the impact on privacy and fundamental rights.

In addition, the Commission has considered the need to avoid any potential abuse or misinterpretation of its recommendations that would result in the exclusion of entire classes of customers and termination of customer relationships, without taking full and proper account of the level of risk within a particular sector.

During the assessment, the Commission has also identified products presenting only a lowly significant (or moderately significant) level of risk for which no further mitigation measures are deemed necessary at this stage. Therefore, measures presented in this report only concern risks that the Commission sees as requiring further mitigation. This approach is meant to allow Member States to better identify priority actions in line with the risk-based approach. Although recommendations for Member States cover many different areas, most relate to the implementation of EU legislation[26]. They were designed to support Member States in focusing on key risk areas when applying their obligations. This assessment does not prejudge the mitigating measures that some Member States are applying or may decide to apply in response to their own national AML/CFT risks. Member States may therefore be implementing some of the recommendations below already or have adopted stricter rules that the minimum rules defined at EU level.

[26] For example national risk assessments, beneficial ownership registers, supervision, resource allocation, feedback for the private sector and sectors at risk of ML/TF which are regulated by 4AMLD

The SNRA seeks to give a snapshot of the ML/TF risks at the time of its publication. This exercise started and ended when the relevant legislative framework in place was Directive 2005/60/EC (3AMLD). Although the 4AMLD had already been adopted at the time, its transposition deadline had not yet passed. For this reason, it was not possible to include any assessment on the concrete effects its implementation would have. However, the changes to the EU's anti-money laundering framework through 4AMLD and proposed amendments to it[27] have been taken into account in defining the mitigating measures, given that these two instruments will substantially strengthen the preventative legal framework and thus mitigate some of the vulnerabilities and risks outlined earlier.

3.1. Mitigating measures under 4AMLD

Under 4AMLD, as of 26 June 2017 the EU legal framework includes new requirements:

- the scope of obliged entities has been extended to cover providers of gambling services, traders accepting cash payments above EUR 10 000 and occasional transactions that constitute a transfer of funds (including money remittances) exceeding EUR 1 000;
- the risk-based approach has been strengthened ;
- registers on beneficial ownership information are put in place to facilitate the identification of beneficial owners of legal entities and some legal arrangements;
- anonymity of e-money products is reduced;
- the new level of sanctions is increasing the deterrent effect;
- a new regime for cooperation between FIUs in the EU is set.

These new measures are expected to decrease risk levels in all sectors substantially. The Commission will review compliance with 4AMLD's provisions and will publish a report assessing implementation by June 2019.

3.2. Mitigating measures already in place or in progress at EU level

In addition, the SNRA has confirmed that more needs to be done on some issues requiring legislative measures or other policy initiatives launched at EU level.

3.2.1. Legislative measures

- **Commission proposal amending 4AMLD**: under this proposal both virtual currencies exchange platforms and wallet providers should become obliged entities to reduce anonymity in transactions. The possibility for electronic money products to be exempted from AML/CFT requirements will be further restricted. The effectiveness of FIUs will be reinforced and centralised bank account registers or retrieval systems will be established to allow better targeted requests. Stricter rules on cooperation between competent authorities, including supervisory authorities, will make for effective information exchange. The nature of the enhanced customer due diligence (CDD) measures to be applied towards high-risk third countries will be further specified to establish a more harmonised approach in that respect. The scope and access of information in beneficial ownership registers will be extended. Furthermore, there are a number of provisions which align the 4AMLD with

[27] COM(2016)450 final

customer due diligence obligations under Directive 2014/107/EU on administrative cooperation on financial account information.

- **Revision of the Cash Control Regulation**[28]: this proposal intends to enable authorities to act on amounts lower than the current declaration threshold of EUR 10000 where there are suspicions of criminal activity, to improve the exchange of information between authorities, and demand disclosure for cash sent in unaccompanied consignments such as postal parcels or freight shipments. The definition of 'cash' would also be extended to include precious commodities acting as highly liquid stores of value such as gold, along with prepaid payment cards.

- The Commission plans to adopt in the summer of 2017 a proposal aiming at combatting terrorism financing via **illicit trafficking in cultural goods** – whatever the country of provenance – to overcome current shortcomings in the art sector[29]. Similarly **wildlife trafficking** is increasingly recognised as a further source of funding of terrorist and related activities[30]. The Commission will continue to implement the EU Action Plan to tackle the illicit financial flows related to wildlife trafficking[31].

- The **Directive on combatting terrorism**[32] includes an EU-wide definition of the crime of financing terrorism and sets minimum rules on the sanctions of this crime. The proposals for a **Directive on countering money laundering by criminal law** [33] and a **Regulation on mutual recognition of freezing and confiscation orders**[34] will also complement the EU preventative approach by ensuring an appropriate law enforcement and judicial response when ML and TF are uncovered.

3.2.2. Policy initiatives

- The Commission is currently looking into launching an initiative to **enhance transparency of cash payments**. It will carry out an impact assessment, taking into account the results of a study and of an open public consultation. The Commission will look at possible options including the possibility of introducing a restriction on cash payments. This could help disrupt the financing of terrorism, as the need to use non-anonymous means of payment would either act as a deterrent against the activity or make it easier to detect and investigate. It could also foster the fight against ML, tax fraud and organised crime. In addition, the decision of the European Central Bank to discontinue production and issuance of EUR 500 banknotes will contribute to further decrease the risk posed by cash payments.

- Based on the EU FIU Platform's above-mentioned **mapping of FIUs' powers and obstacles to cooperation** in December 2016, and on additional analysis, the Commission has outlined possible avenues to improve cooperation of EU FIUs in a separate Staff Working Document listing:

[28] COM (2016) 825 final
[29] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_taxud_004_cultural_goods_synthesis_en.pdf
[30] SWD(2016)38 final
[31] COM (2016) 87 final
[32] COM(2015) 625 final
[33] COM(2016) 826 final
[34] COM(2016) 819 final

- issues that can be resolved through more guidance and enhanced cooperation at the operational level, for example through work at the EU FIU Platform (for instance on standardisation of STR reporting);
- issues that are expected to be resolved once 4AMLD and recent proposed amendments to it have been transposed; and
- other issues originating from divergent legal landscapes in the Member States, which may need to be tackled with regulatory action[35].

The operation of FIUs could be substantially improved with specific EU rules to address issues such as cooperation between FIU and law enforcement authorities at national and EU level. In this respect, the Commission will further examine potential options in line with its Better Regulation principles.

- The Commission has set up an internal **FinTech Task Force** to assess technological developments, technology-enabled services and business models, to determine whether existing rules and policies are fit for purpose and to identify options and proposals for harnessing opportunities or addressing possible risks. Work in this area will cover, in particular, crowdfunding, digital currencies (including crypto-to-crypto transactions and use of virtual currencies for purchasing high value goods), distributor ledger technology and authentication/identification. The use of electronic identification and digital on-boarding will also be analysed. The Commission will carry out a study mapping and analysing on-boarding bank practices across the EU and any next steps will be assessed.

3.2.3. Further supporting measures to mitigate the risk at EU level

- **Improving statistical data collection**: having relevant, reliable and comparable quantitative data at EU level will contribute to a better understanding of the risks. The Commission will therefore aim to improve its statistical data collection on AML/CFT, by collecting, consolidating and analysing the statistics provided by Member States through their obligations under Article 44 of 4AMLD, and by working with Eurostat to increase data comparability.

- **Further guidance to obliged entities on the concept of 'occasional transactions and operations which appear to be linked'**: currently under 3AMLD, obliged entities are required to apply CDD measures when establishing a business relationship or when carrying out an occasional transaction that amounts to EUR 15 000 or more. This notion of 'occasional transactions' makes effective implementation of the rules challenging especially in money remittance and currency exchange services – but also in the gambling sector. Further guidance from the Commission (in cooperation with national competent authorities) would help to mitigate this risk.

- **Training for professionals carrying out activities covered by the legal privilege principle**: they should apply AML/CFT rules more effectively while fully protecting the right to a fair trial and the legitimacy of "legal privilege". Training activities should give operational guidelines and practical insight to help such professionals recognizing operations that may be related to ML or TF and to show them how to proceed in such cases. The Commission will also assess the different options available to improve compliance in this sector in line with of the European Court of Justice case-law[36].

[35] SWD (2017) 275
[36] Case C-305/05

- **Further analysis of risks posed by Hawala and informal value transfer services**: the size of the problem and possible law enforcement solutions should be further analysed. The involvement of law enforcement, especially Europol and Eurojust, together with supervisors is necessary to make deterrent actions against uncooperative actors possible and assist operators wanting to carry out legitimate services in a law-abiding environment.

- **Further work to enhance supervision in the EU**: obliged entities must apply the current rules effectively. Therefore the Commission puts great emphasis on the work carried out by AML/CFT supervisors. There are challenges to be tackled: the large numbers of obliged entities in the EU and their diversity; the volume of transactions and customers; the fragmented landscape of AML/CFT supervisors; and the limitations to supervisors' risk-awareness. Further recommendations will be made to the ESAs and national competent authorities in charge of supervision to ensure that AML/CFT supervisors better understand their role in identifying the risks, and in deciding on the resources to allocate to supervision and on the supervisory actions they should conduct on the obliged entities under their responsibility.

4. RECOMMENDATIONS

4.1. Recommendations for the European Supervisory Authorities (ESAs)

In the financial sector, the ESAs play a pivotal role in raising the EU's capacity to meet the challenges in this sector. The Commission recommends that the ESAs:

- raise awareness as to ML/TF risks and identify the appropriate actions to further build supervisors' capacity in AML/CFT supervision[37]. In that context, they should carry out peer reviews on risk based supervision in practice and identify suitable measures to make AML/CFT supervision more effective;
- take further initiatives to improve cooperation between supervisors. In this respect, the ESAs have recently decided to launch a dedicated work-stream to make the cooperation framework between financial supervisors perform better;
- work out further solutions for supervising operators acting under the "passporting" regime. The European Banking Authority (EBA) joint task force on payment services/anti-money laundering has already started working on this issue. It is seeking to clarify when agents and distributors are actual "establishments" and consider various scenarios that will help address the risks;
- provide updated guidelines on internal governance so as to further clarify expectations around the functions of compliance officers in financial institutions;
- provide further guidance on beneficial ownership identification for investment funds providers, especially in situations presenting a higher risk of ML or TF; and

[37] Risks based supervisory guidelines have been published in November 2016 (https://esas-joint-committee.europa.eu/Publications/Guidelines/Final_RBSGL_for_publication_20161115.pdf)

– analyse operational AML/CFT risks linked to the business/business model in the corporate banking, private banking and institutional investment sectors on the one hand, and in money value transfer services and e-money on the other. This analysis should be carried out in the context of the future joint opinion on risks affecting the financial sector pursuant to Article 6(5) of 4AMLD

4.2. Recommendations for non-financial supervisors

The non-financial sector has no ESA-like EU body or agency in place at EU level. According to the EU's anti-money laundering framework, Member States may allow self-regulatory bodies to perform supervisory functions for tax advisors, auditors, external accountants, , notaries and other independent legal professionals and estate agents. In the large majority of Member States, supervision in these sectors suffers from weaknesses in term of controls, guidance and level of reporting by legal professionals, in particular to the FIU. Therefore, self-regulatory bodies should make efforts to increase the number of thematic inspections and reporting. They should also organise training to develop a better understanding of the risks and AML/CFT compliance obligations.

4.3. Recommendations for Member States[38]

Based on the level of risks identified in the different sectors covered by the SNRA, the Commission recommends that Member States take the mitigating measures below. These should be considered a baseline that could be adapted depending on the national measures already put in place:

- **Scope of national risk assessments**

Member States should give due considerations to the risks posed by the various products in their national risk assessments and define appropriate mitigating measures, particularly on:

- cash-intensive business and payments in cash: Member States should define appropriate mitigating measures such as the introduction of cash limits for payments, cash transaction reporting systems or any other measures suitable for addressing the risk;
- cultural artefacts and antiques: Member States should consider the risk emanating from this sector, promote awareness-raising campaigns among art dealers and encourage them to apply AML/CFT measures;
- NPO sector: Member States should ensure appropriate NPO coverage in their national risk assessments; and
- electronic money products: Member States should take into account the risks posed by anonymous electronic money products and should ensure that the exemption thresholds are as low as possible, to avoid their misuse.

- **Beneficial ownership**

Member States should ensure that the information on the beneficial ownership of legal entities and legal arrangements is adequate, accurate and current.

[38] For more details on the specific recommendations to Member States by products/services see Annex 1 to Staff Working Document (2017)241

(1) Member States should develop adequate tools to ensure that the identification of the beneficial owner is duly undertaken when applying the CDD measures. In the case of legal entities, where obliged entities have identified only the senior manager as the beneficial owner, this should be highlighted by the obliged entity (e.g. through a specific recording of this information). It would be advisable to keep records of any doubt that the person identified is the beneficial owner. Particular attention should be paid to complex structures where the settlor, trustee, protector, beneficiaries or any other natural person exercising ultimate control over the trust involve one or several legal entities.

(2) The rules of 4AMLD on transparency of the beneficial ownership information should also be implemented quickly, with the introduction of beneficial ownership registers for all types of legal entities and legal arrangements. The information in the registers should be verified on a regular basis, for example by a designated authority, so as to avoid discrepancies with information collected by obliged entities as part of their CDD procedures.

(3) Member States should ensure that the sectors the most exposed to risks from opaque beneficial ownership schemes are effectively monitored and supervised. This is particularly the case for intermediaries such as tax advisors, auditors, external accountants, notaries and other independent legal professionals and for providers of advice to undertakings on mergers/acquisitions[39]. In the latter case, while these services are covered by the EU AML/CFT framework, the SNRA highlights ineffective application of the rules to this specific category of undertaking.

- **Appropriate resources for supervisors and FIUs**

In accordance with 4AMLD, Member States must allocate "adequate" resources to their competent authorities[40]. However, from the data collected at this stage, it is not possible to pinpoint any systemic correlation between allocated resources and the size of the sector, the number of obliged entities and the level of reporting. Member States should demonstrate that sufficient resources are allocated to supervisors and FIUs so that they can carry out their tasks.

- **Increase of on-site inspections by supervisors**

In the financial sector, supervisors need to put in place a risk-based supervision model according to the ESAs joint guidelines on risk-based supervision published in November 2016[41]. These guidelines state that supervisors should review – both periodically and on an ad hoc basis – whether their AML/CFT risk-based supervision model delivers the intended outcome and, in particular, whether the level of supervisory resources remains commensurate with the ML/TF risks identified. In this respect, it is important that supervisors conduct sufficient on-site inspections that are commensurate to the ML/TF risks identified.

Member States should ensure that the scope of these on-site inspections is focused on specific operational AML/CFT risks depending on the specific vulnerabilities inherent to

[39] An undertaking other than a credit institution, which carries out activities, listed in point (9) of Annex I to Directive 2013/36/EU.

[40] Articles 32 (3) (on FIUs) and Article 48 (2) (on supervisory authorities) of 4AMLD.

[41] See https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_EN%20%28ESAs%202016%2072%29.pdf

a product or a service. This relates in particular to institutional investment (especially through brokers); to private banking where supervisors should assess the implementation of rules on identifying beneficial ownership; and currency exchange offices and money value transfer services ("MVTS") where supervisory inspections should include a review of training received by agents.

In the non-financial sector, Member States should ensure that their competent authorities conduct sufficient unannounced spot checks on high value dealers especially for gold and diamonds sector to identify possible loopholes in the compliance with CDD requirements. Similarly the number of on-site inspections in the sector of professionals carrying out activities covered by the legal privilege principles should be commensurate to the risks.

- **Supervisory authorities to carry out thematic inspections**

Supervisors should develop a better understanding of the AML/CFT risks to which a specific segment of the business is exposed to. This recommendation should apply to institutional investment (especially through brokers) and private banking; trust and company service providers (TCSPs); tax advisors, auditors, external accountants, notaries and other independent legal professionals; services providers related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings. For those sectors, supervisors should specifically assess the implementation of rules on identifying beneficial ownership. It should also apply to MVTS. In such cases, Member States should ensure that supervisors carry out thematic inspections within 2 years of publication of the SNRA report, unless such inspections have been carried out recently.

- **Considerations for extending the list of obliged entities**

Currently some services/products are not covered by the EU AML/CFT framework. According to Article 4 of 4AMLD, Member States should extend the scope of the AML/CFT regime to professionals particularly at risk. When applying this provision, Member States should consider subjecting at least crowdfunding, virtual currency exchange platforms and wallet providers[42], auction houses, art and antiques dealers and specific traders in high-value goods to their AML/CFT regime, as they are identified as risky under the SNRA.

- **An appropriate level of CDD for occasional transactions**

Based on the current EU legal framework, some services/products may be exempted from CDD for occasional transactions below a specific threshold (EUR 15 000). However, there are some cases where these threshold-based exemptions could be considered as unjustified and where a threshold of EUR 15 000 raises concerns. In that context, Member States should define a lower CDD threshold applicable to occasional transactions to ensure that it is commensurate with the AML/CFT risk identified at national level. Member States should report to the Commission their national threshold for occasional transactions. A threshold similar to that for occasional transactions for transfers of funds can be considered commensurate to the risk (i.e. EUR 1 000). In addition, Member States should provide guidance on the definition of occasional transactions, providing for criteria such that the CDD rules applicable to business

[42] Depending on the outcome of the negotiations on the revision of 4AMLD, virtual currencies exchange platforms and custodian wallet providers could be subject to AML/CFT requirements at EU level.

relationships are not circumvented for currency exchange offices and, pending the new requirements of 4AMLD, money remittances.

- **Appropriate level of CDD in case of safe custody services and similar services**

To monitor safe custody services properly, appropriate safeguards should be put in place. This recommendation should apply to the following sectors:
- safe custody services provided by financial institutions: Member States should ensure that these services are offered only to holders of a bank account in the same obliged entity and should address appropriately risks posed by third-parties access to safe deposit boxes. Guidance should be issued to credit and financial institutions to clarify how they should effectively monitor the content of the safe deposit box as part of their CDD/monitoring requirements; and
- similar storage services provided by non-financial providers: Member States should define measures commensurate with the risks posed in providing these services, including in free-ports, depending on the national circumstances.

- **Regular cooperation between competent authorities and obliged entities**

This enhanced cooperation should seek to make detecting suspicious transactions simpler and to increase the number and the quality of the STRs. Supervisory authorities should provide clear guidance on AML/CFT risks, on CDD, on STR requirements and on how to identify the most relevant indicators to detect ML/TF risks. Member States should ensure that appropriate feedback is delivered by FIUs to obliged entities. This recommendation should apply in particular to the following sectors:
- gambling sector: For gaming machines, clearer guidance should be provided by supervisory authorities on the emerging risk linked to video lotteries. For online gambling, competent authorities responsible should also put in place programmes to raise awareness among online gambling operators as to the emerging risks factors that may impact the vulnerability of the sector. These include the use of anonymous e-money or virtual currency and the emergence of unauthorised online gambling operators; further feedback from FIUs on the quality of the STRs, ways to improve the reporting and about the use made of the information provided, and taking into account specificities of the gambling sector when developing standardisation of STR/SAR template(s) at EU level.
- tax advisors, auditors, external accountants, notaries and other independent legal professionals: Member States should provide guidance on risk factors arising from transactions involving tax advisors, auditors, external accountants, notaries and other independent legal professionals. They should also issue guidance on enforcing the legal privilege and on how to distinguish legal services subject to the very essence of the legal privilege from other services not subject to legal privilege when provided to a single client; and
- MVTS: competent authorities should provide the MVTS sector with further risk awareness and risk indicators on terrorist financing.

- **Special and ongoing training for obliged entities**

Training sessions ensured by competent authorities should cover the risk of infiltration or ownership by organised crime groups. This recommendation should apply to the following sectors:

- gambling sector: for betting, in addition to staff and compliance officers, Member States should envisage mandatory training sessions for betting retailers focused on appropriate risk assessment of their products/business model
- TCSPs, tax advisors, auditors, external accountants, notaries and other independent legal professionals, service providers related to advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings: the training sessions and guidance on risk factors should focus on non-face-to-face business relationships, off-shore professional intermediaries, customers or jurisdictions; and complex/shell structures
- real estate: specific trainings should include red flags for cases where several professionals are involved in the real estate transaction (estate agent, legal professional, financial institution); and
- MVTS: obliged entities should provide mandatory trainings to agents to make them aware of their AML/CFT obligations and show them how to detect suspicious transactions.

- **Annual reporting from competent authorities/self-regulatory bodies on the AML/CFT activities of the obliged entities under their responsibilities.**

This reporting obligation will help national authorities conduct their national risk assessments and allow for more proactive actions to deal with weaknesses or failures to comply with AML/CFT requirements in the following sectors:
- real estate: the report should include the number of reports received by the self-regulatory body and the number of reports transmitted to the FIUs when those professionals are reporting via a self-regulatory body; and
- tax advisors, auditors, external accountants, notaries and other independent legal professionals: the report should include the number of on-site inspections carries out by self-regulatory bodies to monitor AML/CFT compliance, the number of reports received by the self-regulatory body and the number of reports transmitted to the FIUs when those professionals are reporting via a self-regulatory body.

5. CONCLUSIONS

The SNRA shows that the EU internal market is still vulnerable to ML/TF risks. Terrorists use a wide range of methods to raise and move funds and criminals employ more complex schemes and take advantage of new opportunities to launder money offered by the appearance of new services and products. Preventing the misuse of the financial system is crucial to limit the capacity of terrorists and criminals to operate and to deprive organised crime of the economic benefits which are the ultimate goal of their illegal activities.

The solid assessment carried out in the last two years has highlighted the need to refine certain elements of the legislative framework and strengthen the capacities of public and private actors to implement their compliance obligations.

Some measures are already being pursued, and the Commission will implement new measures outlined in this report to mitigate the risks appropriately. The Commission invites Member States to implement the recommendations issued in this report expediently. Under Article 6 of 4AMLD, Member States that decide not to apply any recommendations in their national AML/CFT regimes, should notify the Commission of

their decision and provide a justification for it ("comply or explain"). In the absence of such notifications, Member States are expected to implement those recommendations.

In order to be effective AML/CFT policies should adapt to the development of the financial services, the evolution of the threat and the emergence of new risks. For this reason, the Commission will monitor the actions taken by Member States based on the SNRA findings and report on these findings at the latest by June 2019. That review will also assess how measures implemented at EU and national level impact on risks level. Faced with an evolving challenge which profits from any new loophole, all actors must remain vigilant and increase their efforts and cooperation: concerted action is more necessary than ever to combat money laundering and terrorism financing and thus reinforce the stability of the internal market and improve the security of EU citizens and society as a whole.