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

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.