



Online Gambling

MONEYVAL

RESEARCH REPORT

**The use of online gambling for money laundering
and the financing of terrorism purposes**

April 2013

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

www.coe.int/moneyval

The use of online gambling for money laundering and the financing of terrorism purposes¹

¹ Ref. MONEYVAL(2013)9, dated 11 April 2013, adopted by MONEYVAL at its 41st plenary meeting (8-12 April 2013)

Table of Contents

1. Introduction	6
2. Situation in MONEYVAL Member States	7
2.1 Overview of the online gambling sector	7
2.2 Regulatory framework in the online gambling sector	7
2.2.1 Licensing systems	7
2.2.2 AML/CFT obligations upon online gambling operators	7
2.2.2 AML/CFT regulation of payment and other payments requirements	7
2.2.4 Requirements to open an e-account	8
2.2.5 Verification of information by the licence holder	8
2.2.6 Payment options	8
2.3 Extent and type of gambling offered and policy position	8
3. ML/FT risks through online gambling	10
3.1 Typologies	10
3.2 Red-flag Indicators	11
3.3 Vulnerabilities	12
3.3.1 Vulnerabilities related to online gambling	12
3.3.2 Vulnerabilities related to the methods of payment used for online gambling	13
3.3.3. Issues faced by law enforcement authorities	14
4. Conclusions	15

Abbreviations and Acronyms

AML/CFT	Anti-Money laundering and countering the financing of terrorism
CDD	Customer Due Diligence
DNS	Domain Name System
EU	European Union
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FT	Financing of Terrorism
ISP	Internet Service Providers
IP	Internet Protocol
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of anti-money laundering measures and the financing of terrorism
RBA	Risk-Based Approach

1. INTRODUCTION

1. In recent years the online gambling industry has experienced a boom. This is largely the result of ever-evolving technological developments, which have enhanced the online gambling experience and made it very easily accessible. The volume of online gambling has increased tremendously and the sector now accounts for significant financial volumes.

2. Online gambling is intrinsically a cross-border activity. The different components involved in the operation of a gambling website are generally situated in different locations around the world, including offshore jurisdictions. For instance, an online gambling website may be registered in one jurisdiction, while the server may be located in another. The financial activity and management of the online gambling operation may be situated in yet another jurisdiction. As a result, multiple stakeholders and legal systems are involved in the regulation of the sector, giving rise to possible legal and jurisdictional gaps which may be misused for ML/FT purposes.

3. The online gambling sector faces other challenges in managing the risk of ML/FT. In particular, the emergence of alternative payment systems to deposit funds into online gambling accounts may have a significant impact on the exposure of online gambling to ML/FT risks. Furthermore, as a result of the high turnovers generated by online gambling and the ease with which an online gambling operation may be set up in certain jurisdictions, the sector has become particularly attractive to criminal organisations as a means to launder funds derived from criminal activities. These and other vulnerabilities will be explored in greater detail in this report.

4. Criminal activity within the online gambling sector extends to other areas beyond ML/FT. The most common criminal threats which are often connected to this sector are primarily fraud and match-fixing. Although a direct link exists between these activities and money laundering, the methodologies used by criminals in perpetrating these activities do not fall within the scope of this study and will therefore not be examined in the report.

5. In March 2009, the FATF and the APG jointly published a typologies report on ML/FT through the casino sector². Although the report does not seek to examine the risks linked to online gambling, reference was made to the significant gap that exists in the identification and analysis of ML/FT risks and vulnerabilities within the online gambling sector. It was acknowledged that additional typologies research on ML/FT through online gambling was needed.

6. In this spirit, a decision was taken by MONEYVAL to conduct a typologies study to shed some light on any possible ML/FT typologies, vulnerabilities and indicators within the online gambling sector. The study was conducted by a team comprising two representatives from the FIU of Cyprus (MOKAS), who led the team, a representative from the FIU of Romania (NOCPML), a representative from the FIU of Israel (IMPA), a representative from the FIU of Malta (FIAU) and a representative from the MONEYVAL Secretariat.

7. The study was based on information gathered from two questionnaires distributed to MONEYVAL members and observers, a typologies meeting held in Limassol, Cyprus (November 2009) and a supplementary meeting with representatives from the public and private sector held in St. Julian's, Malta (May 2011). Publicly-available literature was also consulted.

8. Since limited information was made available to the project team by MONEYVAL members, it was only possible to provide a generic view of the size, nature and volume of the online gambling sector and the manner in which it is regulated. The same applies to the analysis of ML/FT risk within the sector.

² Vulnerabilities of Casinos and Gaming Sector, APG (Asia Pacific Group on Money Laundering) and FATF Report, March 2009.

2. SITUATION IN MONEYVAL MEMBER STATES

2.1 Overview of the online gambling sector

9. It is difficult to provide a description of the online gambling environment in MONEYVAL member states since very limited information was made available. Nevertheless, three different categories of jurisdictions may be identified:

- Jurisdictions where online gambling is both legal and regulated. Such jurisdictions may serve as hosts for online gambling infrastructure, thus enabling online sites to offer their services in other countries around the world. The level of regulation varies between the different jurisdictions falling within this category.
- Jurisdictions where online gambling is legal but not regulated. Such jurisdictions may pose a risk by allowing the registration of online gambling sites without proper supervision, including the risk of using the online gambling infrastructure to launder illicit funds or to finance terrorism.
- Jurisdictions where online gambling is illegal. This activity may also constitute a predicate offence for ML purposes and thus any funds generated through online gambling would be considered illicit property. Some of the jurisdictions within this category pointed out that, even though online gambling is illegal within their territory, online gambling websites have developed ways to evade restrictions or limitations put on their financial activity by, for instance, providing a false clearing code for credit card transactions to enable the gambling activity to be cleared by the local credit card companies.

2.2 Regulatory framework in the online gambling sector

2.2.1 Licensing systems

10. The conditions for the issuance of an online gambling licence are largely similar in all MONEYVAL member states where a licensing system is in place. Generally, an application for an online gambling licence must be submitted by a legal entity registered in the country where the licence is being applied for. The managing board of the legal entity applying for the licence is required to fulfil certain 'fit and proper' criteria and the identity of beneficial owners controlling the legal entity must be disclosed. Detailed technical requirements on control and gambling systems also generally apply in all countries. The authorities responsible for issuing online gambling licences and for the supervision of licensed operators vary according to the country. These include ministries of finance, tax authorities and gambling authorities.

2.2.2 AML/CFT obligations upon online gambling operators

11. Licensed online gambling operators generally fall within the scope of the national AML/CFT legislation and are therefore subject to CDD, record-keeping and reporting requirements. Supervision for AML/CFT purposes is either conducted by the FIU or else by the financial/gambling supervisory authority of the country concerned.

2.2.2 AML/CFT regulation of payment and other payments requirements

12. Most MONEYVAL members which regulate online gambling have measures in place to ensure that online gambling operators licensed within their jurisdiction only accept payments from licensed credit and other financial institutions which are subject to adequate AML/CFT obligations. In certain countries, transactions conducted between the online gambling operator and the player may only take place through a special purpose account. In other countries, online gambling

operators may only receive payments from a credit or financial institution which is licensed in that country.

13. In most legal systems, online gambling operators must ensure that funds in a gambling account are credited to the same account from which the funds were initially deposited. This ensures that no payments are made from the account of the player to third parties.

14. Online gambling operators are, in the large part, also required to maintain players' funds separately from their own funds in a clients' account held with a credit institution. Such accounts are subject to on-going monitoring by the credit institution which provides an added layer of scrutiny over the transactions carried out through such an account.

2.2.4 Requirements to open an e-account

15. Online gambling operators are required to open an account for each player upon registration. Registration consists of the identification of the player, which includes the full name, date of birth and address of the player. In some cases an identification number, the email address and the tax number of the player are also requested. It is not clear whether all countries require e-accounts to be linked with at least one bank account in the name of the player.

16. Restrictions with respect to the age of the player vary from one country to the other. In some countries persons under the age of eighteen years are prohibited from opening an account, while in other cases the age limit is twenty one years.

17. Other restrictions exist:

- limitations on the amount of money that can be gambled;
- limitations as to the amount of time that can be spent gambling;
- restrictions on the number of gambling accounts that can be held by a player (which is usually one per player);
- prohibition to provide credit to a player;
- prohibition to accept stakes from a player if no funds stand to credit of the player.

2.2.5 Verification of information by the licence holder

18. The verification of identity of players generally takes place through the use of commercial websites providing such services. In certain countries online gambling operators are required to carry out face-to-face verification of identity as the opening of an e-account falls within the definition of a business relationship in terms of AML/CFT law.

2.2.6 Payment options

19. Various payment methods can be used to fund online gambling accounts; debit/credit cards, online payment providers, wire transfers, e-cash, cheques and pre-paid cards. Deposit of funds by means of debit/credit cards is an acceptable form of payment in all countries. Online payment providers and wire transfers are also commonly acceptable forms of payments, although to a much lesser extent than debit and credit cards. E-cash, cheques, cash and prepaid cards are not generally permitted as methods of payment.

2.3 Extent and type of gambling offered and policy position

20. The overall number of licensed online gambling operators and websites does not appear to be extensive within MONEYVAL member states, with the exception of a small number of countries. In some countries the single licence concept³ applies. The type of online gambling that is provided is betting, casinos and lotteries/bingo. On the basis of information provided in the questionnaires, MONEYVAL members may be roughly placed into four different categories. The first category consists of those jurisdictions where the number of licensed entities and websites operated by such entities is substantial and all types of online gambling websites are available. In the second

³ The single license concept applies in those jurisdictions which confer exclusive rights on a single operator (set up either under public or private law) to provide gambling services, and whereby all other operators are prohibited from providing gambling services in that jurisdiction.

category, there are those jurisdictions in which the single licence concept applies or the number of licensed entities and type of online gambling websites which are available is very limited. The third category comprises those jurisdictions where all types of online gambling websites are available but the number of licensed entities and websites is very low. In the fourth category only sports betting is available. However, the number of licensed entities and websites in these jurisdictions is quite substantial.

21. The distinction between these categories does not seem to have any bearing on the restrictions imposed by these jurisdictions with respect to the provision of online gambling. In fact, while in certain jurisdictions operators licensed in another jurisdiction are not allowed to operate domestically and cross-border online gambling is not permitted, in other jurisdictions operators licensed in other jurisdictions are allowed to provide their services insofar as they are licensed in their country of origin or have received permission to provide their services by the foreign jurisdiction. These variances contribute further to the diversity of the online gambling environment in MONEYVAL members.

22. Measures are being undertaken by all jurisdictions regulating online gambling to ensure that the sector is subject to appropriate safeguards and to prevent the provision of illegal gambling, which, as was reported, generally originates from offshore jurisdictions or certain Asian countries. In order to detect and prevent illegal gambling, various techniques are used. For instance, in one case the gambling authority is empowered to request the blocking of certain websites related to online gambling, where the appropriate authorisation has not been obtained. In another case a similar system of IP blocking is used to prevent illegal online gambling websites and the ISP may be obliged by the gambling authority to block the domain name of illegal online gambling operators. A list of the websites which have been blocked by order of the gambling authority is in these circumstances usually publicly available on the authority's website and any person attempting to access a listed website would be redirected to a "landing page" of the gambling authority. The authorities of another country reported that the gambling authority has set up an IT-prevention section which focuses on detecting unlicensed operators and any activities which are detected are immediately reported to the police. In one country when the gambling authority detects the operation of an unlicensed activity, a prohibition order is issued. Where such prohibition order is not observed, an application may be made to the administrative courts to issue an order to the IP providers to block the access to such unlicensed websites. It was reported that in practice the filtering of DNS is used in order to block access to such websites.

3. ML/FT RISKS THROUGH ONLINE GAMBLING

23. The information provided by MONEYVAL members on ML/FT risks within the online gambling sector in response to the questionnaires was very limited. It is therefore difficult to determine the extent to which the online gambling sector is vulnerable to the risk of ML/FT within MONEYVAL member states. This also appears to be the case within the member states of the European Union. As indicated in the European Commission Staff Working Document on Online gambling in the Internal Market⁴, issued on 23 October 2012, there is currently very limited information or evidence suggesting that licensed online gambling operators in Europe are being misused for ML/FT purposes.

24. Furthermore, various sources of literature on the topic⁵, which were consulted by the project team, seem to indicate that the ML/FT risks linked to regulated online gambling are low and that the sector is not likely to be the preferred option for money launderers or terrorist financiers due to the following factors:

- gamblers are subject to customer identification controls and therefore their identity is known;
- financial transactions related to online gambling are conducted electronically and are therefore easily traceable;
- all wagering carried out by online gambling operators is recorded.

25. Nevertheless, the absence of any significant information on concrete ML/FT cases should not be construed to mean that the risk of ML/FT within the online gambling sector does not exist. Indeed, in the course of the workshop held with various representatives of FIUs, supervisory authorities and law enforcement authorities and the supplementary meeting held with supervisory authorities and private sector representatives, various potential ML/FT typologies, red-flag indicators and vulnerabilities were identified. These typologies, indicators and vulnerabilities are not based on empirical data or hard evidence but on the experiences and anecdotal information shared by public and private stakeholders with the project team. The conclusions of the project team also build upon the ML/FT risks identified by the FATF in the RBA Guidance for Casinos⁶ in relation to remote casinos.

3.1 Typologies

26. The following potential typologies were identified by the project team:

- A money launderer, in collusion with an operator of an offshore gambling website, deposits funds obtained from criminal activities in the gambling account and withdraws such funds as winnings. The website operator keeps a percentage of the proceeds as a commission while the launderer declares the winnings to the tax authorities and then uses the funds for legitimate purposes.
- A money launderer sets up a company in an offshore jurisdiction through various frontmen. The company then applies for an online gambling licence in the offshore jurisdiction. Funds deriving from criminal activity are then laundered through the online gambling website which is controlled by the launderer.
- A criminal colludes with other persons who act as beneficial owners of a company which is used to obtain an online gambling licence. Illegally obtained funds are then co-mingled with the legitimate profits of the company and deposited in a bank account.
- A money launderer sets up an online gambling website without registering the website or obtaining a licence. The website is not made available to the public but is used to place

⁴ SWD(2012) 345 final P.89

⁵ 'The threat of money laundering and terrorist financing through the online gambling industry' prepared by MHA Consulting for the Remote Gambling Association (June 2009) and 'Money laundering risks and E-Gaming: A European overview and assessment', Michael Levi (September 2009)

⁶ FATF RBA Guidance for Casinos 23 October 2008

funds obtained from criminal activities which are then distributed as winnings to various frontmen. The website is then disconnected citing failure to make a profit as the primary reason for the disconnection.

- A money launderer colludes with professional gamblers to place illegally obtained funds on online gambling websites. The gamblers keep a commission from any winnings made before transferring the remaining funds to the launderer.
- Illegally obtained funds are deposited into an online gambling account using a false identity. The player engages in minimal gambling activity which is sufficient to make the account appear genuine. After incurring minimal losses the funds are then transferred from the gambling account to a legitimate bank account.
- A money launderer deposits funds derived from criminal activities into an e-wallet through a money service business. The funds are then deposited into an online gambling account by frontmen. The winnings are remitted back to the e-wallet account and used for other legitimate purposes on other websites.
- A money launderer deposits funds into an online gambling account by using a stolen identity to avoid detection.
- Peer-to-peer games such as e-poker, where value transfers can occur between both electronic and human players as a result of deliberate losses, at a relatively low cost to the players. Players will make large bets on very bad hands expecting to lose to the accomplice.⁷ This is generally known as chip-dumping and is considered to mainly pose a risk of FT.

3.2 Red-flag Indicators

27. The project team found the following red-flag indicators of possible laundering through online gambling:

- Information provided by the player contains a number of mismatches (e.g. email domain, telephone or postcode details do not correspond to the country);
- The registered credit card or bank account details do not match the player's registration details;
- The player is situated in a higher-risk jurisdiction or is identified as being listed on an international sanctions list;
- The player is identified as a politically exposed person;
- The player seeks to open multiple accounts under the same name;
- The player opens several accounts under different names using the same IP address;
- The withdrawals from the account are not commensurate with the conduct of the account, such as for instance where the player makes numerous withdrawals without engaging in significant gambling activity;
- The player deposits large amounts of funds into his online gambling account;
- The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds;
- The customer logs on to the account from multiple countries;
- A deposit of substantial funds followed by very limited activity;
- The player has links to previously investigated accounts;
- Different players are identified as sharing bank accounts from which deposits or withdrawals are made.

⁷ Staff Working Document P. 91

3.3 Vulnerabilities

3.3.1 Vulnerabilities related to online gambling

28. Following discussions with stakeholders, it was noted that the ML/FT risk is significantly increased when online gambling is conducted through offshore jurisdictions or jurisdictions that do not regulate online gambling. This is due to the fact that, in such cases, supervision and regulation are completely absent and no preventive measures are applied to players. This conclusion is broadly in line with the findings of the EU Commission, which links ML/FT risks primarily to “unregulated operators who are offering their services at a distance from outside of the EU with either no or a very low degree of regulation and supervision”.⁸

29. The main vulnerabilities identified by the project team were the following:

- **The cross-border nature of online gambling**
In view of the fact that online gambling has a cross-border element, it may be subject to different regulatory regimes. This can create regulatory gaps which may be abused of by criminals. In such circumstances, there is no structured and systematic cooperation between supervisory authorities and law enforcement authorities situated in different jurisdictions.
- **The rapidity and cross-border nature of transactions⁹**
Since online gambling transactions are conducted over the internet, tracing such transactions and linking them to specific individuals may prove problematic in certain instances.
- **Non face-to-face nature of online gambling**
The fact that players are not physically present for verification of identity purposes renders the CDD procedure more complex.
- **Low number of investigations and prosecutions of ML/FT cases**
Law enforcement authorities and prosecutors have limited exposure to and knowledge of the manner in which criminals may misuse online gambling for ML/FT purposes. It is therefore difficult to train law enforcement and prosecution authorities on the ML/FT typologies used in this sector.
- **Crediting winnings to different accounts**
Online gambling operators, especially those which are unlicensed, that credit winnings or unused funds to an account other than the account through which funds were originally deposited into the gambling account, may unwittingly launder illegally obtained funds. Although licensed online gambling operators are not permitted to perform such operations, difficulties may arise when funds are initially deposited through, for instance, a Mastercard account which does not allow for inward transfers of funds.
- **Use of multiple accounts**
Online gambling operators which permit players to set up multiple accounts enable customers to move funds freely between different accounts, thereby obscuring the origin of the funds.
- **The use of money service businesses**
Money service businesses generally accept cash in order to credit internet gambling accounts. The use of cash in this case creates difficulties in tracing the origin of the cash, especially if the MSB concerned does not apply adequate CDD measures.
- **The use of Master Accounts**
An online gambling master account is made available to a person offering gambling activities from an establishment. Players of the establishment are provided with direct access to the master account without being subject to any CDD measures. Under these

⁸ Ibid. P. 89

⁹ To some extent this vulnerability is in conflict with the findings in the MHA Consulting report mentioned earlier in the report, which states that the risk of ML/FT through online gambling is minimised since financial transactions related to online gambling are conducted electronically and are therefore easily traceable.

circumstances, the provider of the master account is not in a position to identify the individual players who utilise the master account.

- **V.I.P. Accounts**

Online gambling operators might provide V.I.P. accounts to certain players who place large deposits of funds in their gambling account. These players are generally not subject to strict CDD procedures.

- **Mixed gambling chains**

Players deposit cash through land-based gambling operators and transfer the funds to an online gambling account. In this manner the use of the financial system is circumvented completely.

3.3.2 Vulnerabilities related to the methods of payment used for online gambling

30. It may be argued that, since online gambling transactions are primarily conducted through the financial sector, an added layer of preventive measures ensures that ML/FT activities are detected, thereby reducing the ML/FT risk considerably. However, there are various factors which militate against this assumption:

- Banks are not in a position to identify every possible ML/FT suspicion related to a player, since they do not have access to certain information on the player, such as for instance the gambling pattern of the player;
- Unlicensed online gambling sites do not require players to deposit funds through licensed financial institutions which are subject to adequate AML/CFT requirements;
- Not all jurisdictions that licence online gambling require online gambling operators to ensure that players deposit funds solely through licensed financial institutions which are subject to adequate AML/CFT requirements.

31. Another important factor which needs to be taken into consideration when assessing the risk of ML/FT within the online gambling sector is the use of alternative payment methods to deposit funds into an online gambling account. Methods of payment are generally classified as traditional and alternative methods. Traditional methods include bank accounts (wire transfers), debit and credit cards, travellers' cheques, bank drafts and personal cheques and money remittances. Alternative methods comprise pre-paid cards, online payment providers and digital currency (E-cash).

32. According to representatives from the online gambling sector, since financial institutions are increasingly blocking credit card transactions related to online gambling, it is expected that the demand for alternative payment methods will increase. It is therefore essential for online gambling operators to ensure that players deposit funds through regulated entities providing alternative payment services which are subject to adequate AML/CFT measures. The ML/FT risks associated with alternative payment methods have already been explored in detail by the FATF. For a thorough understanding of these risks reference should be made to the various FATF reports¹⁰ issued in relation to this topic.

33. With respect to online gambling, two major vulnerabilities were identified by the project team in relation to alternative payment methods:

- **Deposit of funds through financial intermediaries**

The use of online financial intermediaries that are not subject to adequate AML/CFT regulation to deposit funds into a gambling account make it impossible to identify the source of funds deposited into a gambling account.

¹⁰ FATF typology reports: "Report On New Payment Methods" October 13, 2006; "Money Laundering & Terrorist Financing Vulnerabilities Of Commercial Websites And Internet Payment Systems", June 18 2008 and "Money Laundering Using New Payment Methods" October 2010

- **The use of prepaid cards**

The use of prepaid cards which are subject to lighter CDD requirements to deposit funds in a gambling account makes it difficult for online gambling operators to identify the source of funds.

3.3.3. Issues faced by law enforcement authorities

34. As mentioned in previous parts of the report, the regulation of online gambling differs considerably in MONEYVAL member states. These differences may hinder effective law enforcement co-operation and cross-border investigations. For instance, in view of the fact that online gambling is considered legal in certain countries while illegal in others, difficulties arise in the collection of evidence through mutual legal assistance. Furthermore, investigators face challenges due the nature of the operational set-up of online gambling. For instance, servers might be located in one jurisdiction while management of the sites could take place remotely from other jurisdictions. At the same time gamblers can access these sites from anywhere around the globe. Identifying all these different locations through an IP address is a complex process for law enforcement, especially in those cases where an unlicensed online gambling website is involved.

4. CONCLUSIONS

35. The online gambling sector within MONEYVAL member states is fairly diverse. In some jurisdictions, online gambling is legal and subject to regulations. In other jurisdictions, although online gambling is not prohibited, no supervisory framework exists to regulate the sector. In a few jurisdictions, online gambling is considered illegal and persons engaging in such activities are subject to criminal sanctions.

36. The extent of online gambling within MONEYVAL member states varies significantly. Few jurisdictions have issued an extensive number of licences to online gambling operators. In certain jurisdictions the single-licence concept applies. The type of online gambling offered is generally betting, casinos and lotteries/bingo.

37. In those jurisdictions where a regulatory framework exists, licensing systems are broadly homogenous. 'Fit and proper' criteria are applied to the management of an applicant for a licence and information on the beneficial owners of the gambling operation is required to be disclosed before a licence is issued. Various licence conditions are applied to licence holders. Additionally, all online gambling operators are required to comply with AML/CFT requirements.

38. Where there are requirements on the means of payment to be used for gambling purposes, they are similar; payments may only be accepted from licensed financial institutions. All jurisdictions require online gambling operators to open e-accounts for players. However, the conditions for the opening of such accounts and the restrictions imposed on the operation of such accounts vary.

39. All the jurisdictions which regulate online gambling have reported that efforts are made to supervise and safeguard the sector through various measures, such as for instance IP blocking.

40. Information on ML/FT risks in the online gambling sector, both within MONEYVAL and European Union member states, is limited.

41. Studies on this topic conducted by private researchers seem to indicate that the ML/FT risks linked to regulated online gambling are low and the sector is not likely to be the preferred option for money launderers or terrorist financiers. This is broadly in line with the conclusion reached by the European Commission after conducting a study of online gambling in the internal market. It was concluded that there is very limited information or evidence suggesting that licensed online gambling operators in Europe are being misused for ML/FT purposes.

42. Nevertheless, on the basis of anecdotal information shared by public and private stakeholders with the MONEYVAL project team, a number of vulnerabilities, red-flag indicators and typologies related to the online gambling sector were identified.

43. One of the major vulnerabilities appears to be directly linked to unregulated online gambling. In an environment where the operation of online gambling is not subject to a supervisory framework, the susceptibility to abuse increases drastically. It is easy for criminals to infiltrate the sector or to manipulate online gambling operations for illegal purposes, in the absence of adequate control systems.

44. Given that online gambling, by its nature, is conducted anonymously, the use of false or stolen identities by criminals is less likely to be detected. Collusion between different players for the purpose of value transfer between different accounts is also facilitated.

45. The use of alternative payment systems to credit online gambling accounts systems may also augment the risk of ML/FT. Accepting payments through such systems should therefore be subject to the strictest level of controls by online gambling operators.

46. Challenges also arise due to the cross-border nature of online gambling. As discussed in the report, variances in the regulatory frameworks within different jurisdictions and the fact that many countries do not regulate online gambling at all can create gaps which may potentially be misused by criminals.

47. The regulation and supervision of online gambling is therefore one of the strongest mitigating factors to prevent abuse. Regulating online gambling can minimise ML/FT risks where:

- persons wishing to set up online gambling operations are subject to scrutiny by licensing authorities thereby decreasing the risk of criminal elements infiltrating the sector;
- online gambling operators are required to apply AML/CFT preventive measures to detect and report abuse;

- online gambling is permitted only where funds are transferred through regulated financial institutions.

48. Other measures that may be imposed on online gambling operators to reduce ML/FT risks are the following:

- Prohibiting the registration of multiple accounts;
- Restricting inter-account transfers;
- Requiring winnings to be credited to the accounts held only in the name of the player;
- Restricting third party payments from online gambling accounts;
- Restricting deposits of cash through mixed land-based and online gambling chains.

www.coe.int/moneyval