

Review of the 3rd AML directive: Solicitation of stakeholder views Deadline for comments 3rd October 2011

Introduction

The European Gaming and Betting Association (EGBA)¹ is pleased to submit its views on the review of the 3rd AML directive. The EGBA represents the leading online gaming and betting operators established, licensed and regulated within the EU. Our members offer services online such as sports betting, poker, casino, bingo and backgammon. All EGBA members comply with a set of strict rules in terms of governance and account control. Some of our members are publicly listed companies.

Executive summary

- EGBA members fully support the principles of the 3rd AML directive and already apply AML provisions as part of their national licensing regime(s).
- Evidence shows that the risks of money laundering in the online provision of gambling services are lower than in the offline environment due to the traceability and transparency of internet transactions².
- In addition, the generally low value of transactions in the online sector means that a risk based approach is preferable rather than a one size fits all KYC approach that is identical for both online and offline gambling services.
- KYC measures for online gambling services should be adapted to reflect the different characteristics of online and offline gambling services provision and their respective risks.
- In order to apply all 3rd AML requirements to online, the sector should be able to have access to all available instruments that allow ID verification.
- EGBA members support the review of the 3rd AML directive with the view to clarifying the scope of the directive and recognising that there are tools that are fully adapted to information society services including online gambling services.

1. To what extent do you consider it appropriate to introduce a more risk based approach into the 3rd AML and do you believe this should be done?

EGBA members strongly support a risk based approach to ensure efficiency and effectiveness of the measures taken. It is especially important to take into account the specific characteristics of the online gaming industry and evaluate the risk accordingly. Examples of this are the general low value of transactions (a Bwin customer makes on

¹ <http://www.eu-ba.org/en/>

² http://ec.europa.eu/internal_market/services/docs/gambling/workshops/workshop-iv-conclusions_en.pdf

average 4 bets a week at €4 each for sports bets) as well as the fact that all transactions are done through regulated financial institutions and never in cash. Effectively targeting the high risk areas will increase the effect of the measures, rather than spreading the measures thin or applying a one-size-fits-all approach.

2. Can you provide any evidence which might support a case for a more focused approach to the application of AML/CFT rules, or outline the ways in which this might be achieved in the case of smaller businesses, in particular which might support the claim for greater effectiveness?

First of all, when it comes to reporting and intelligence gathering a focused approach is per definition needed, as the aim is to separate and identify patterns with high risk from those with low risk. Reporting each single transaction of each single client in an unfocused manner is obviously useless.

Stringently, those transactions and clients with a very high risk should naturally be put under considerably bigger scrutiny (CDD etc), than those with very low or zero risk. By using the same amount of resources a focused approach, whereby those resources are applied in relation to the risk, will always have far superior effect per resource than an approach whereby considerable resources are spent unnecessarily on clients and transactions bearing no risk. This approach also allows more rigid controls without distorting the commercial possibilities and thereby the efficiency of the market as such.

3. What is your assessment of the risk associated with customer identification in non face to face situations?

The risk associated with customer identification in a regulated environment for online gambling is minimal³. This is due to the transparency of the internet which allows in a regulated environment to make all transactions traceable from when a customer signs up, up to when he cashes out. This is done thanks to sophisticated checks which are part of the requirements of the third AML and specific to the online gambling industry. To prevent fraud, our members will, for instance, monitor a number of characteristics such as:

- Deposits of substantial sums (initial and ongoing)
- Deposits not immediately used as stakes in betting
- Deposits and withdrawals made without placing any bets

If one or more characteristics of suspicious behaviour are detected alerts are being triggered that lead to detailed investigations of accounts and customers (Enhanced Due Diligence) and could lead to Suspicious Activity Reports issued by nominated Money Laundry Reporting Officers.

4. Do the risks differ from face to face situations?

³ http://www.egba.eu/pdf/Levi_Final_Money_Laundering_Risks_egaming%20280909.pdf

As stated in the European Commission Green Paper on online gambling⁴ *“On-line gambling provides operators with more sophisticated possibilities to track the transactions of each player compared to off-line gambling formats”*.

This view was further confirmed in the most recent conclusions of the European Commission workshop⁵ on online gambling on the prevention of fraud and money laundering, where it stated *“customers are not anonymous, operators create detailed identification profiles and carry out due diligence controls which enables the tracking of suspicious gambling patterns (including money flows and destination of these) to be traced back to the individual player”*.

It is a fact that in a regulated online gambling environment, internet transactions are traceable and transparent and hence offer more possibilities than in land based environment. There are indeed no cash transactions involved. A large majority of deposits and withdrawals⁶ (65%) are made via highly regulated financial institutions such as banks or credit card companies.

In an offline environment, the same scenario is almost impossible to reconstruct. This implies that the risks are many fold. For instance, in terms of fraud – money laundering, one can walk and spend a high level amount of cash into a betting shop or casino and walk away. In terms of age controls, the following mystery shopping exercises show as well that online age controls are more efficient than offline *‘face-to-face’* identification:

- A UK Gambling Commission mystery shopping exercise conducted in 2009⁷ revealed that while 95% of online players had registered with operators that had no weaknesses in their underage gambling procedures, 98% of betting land-based shops allowed underage individuals to place a bet at the counter.
- A mystery shopping exercise conducted in 2009⁸ by the Belgian consumer organisation (CRIOC) also revealed the lack of enforcement of age restrictions in the offline gambling market with an impressive rate of 71% of offline points of sale which were found selling illegally lottery tickets to minors.

5. Do they justify the application of enhanced due diligence (art 13.2 of the 3rd AML)?

EGBA members already apply enhanced due diligence as part of any national licensing regime or general AML provisions and hence are fit to apply a risk based approach for non face to face transactions. It is however important to acknowledge the difference risk level as most transactions are done via a regulated financial institution and never directly with

⁴ http://ec.europa.eu/internal_market/consultations/docs/2011/online_gambling/com2011_128_en.pdf page 22

⁵ http://ec.europa.eu/internal_market/services/docs/gambling/workshops/workshop-iv-conclusions_en.pdf

⁶ http://ec.europa.eu/internal_market/consultations/docs/2011/online_gambling/com2011_128_en.pdf, page 17

⁷ <http://www.gamblingcommission.gov.uk/pdf/online%20mystery%20shopping%20programme%20july%202009.pdf>

⁸ <http://www.crioc.be/FR/doc/x/y/document-4434.html>

the clients. Also, the actual CDD measures should include the unique possibilities that the online sector offers. As highlighted above, internet offers more opportunities than the offline environment to detect suspicious activities, something the current CDD requirements don't fully make use of.

6. Can you provide evidence of how such risks are managed by online operators?

The following list is not exclusive but shall give an overview of the controls and checks that are possible in a regulated online gambling environment:

- Identification of issuer countries of credit cards: This enables operators to check whether the country of origin indicated by the customer upon registration matches with the payment method.
- Cross-check of customer's IP location with country of origin: This is to check whether the customer is actually located in the country indicated to be the country of origin during registration.
- Check whether the same credit card or e-wallet account is used for deposits and/or withdrawals of more than one customer account: This could be an indicator of one customer having more than one gaming account.
- Check for critical mix of payment methods, especially anonymous scratch-cards or payment services regulated outside of the EU: This could be a potential indicator that the player attempts to hide the origin of the funds.
- Check customer database against lists of politically exposed persons: Attempts by such individuals to open gaming accounts have to be reported to the Money Laundry Reporting Officer (MLRO) in a first step and to the relevant financial investigation units in a second step.

7. How would you suggest the current rules might be adjusted in order to bring them more in line with market developments?

The rules should take into consideration that operators can evaluate the ML risk of their customers based on the products they use, frequency, value of deposits, origin of deposits, risk level per payment method and payment country and last but not least monitor for significant changes in customer paying and playing behaviour. As outlined above, online operators do have a full audit trail of all their customer activity and by this can define precise player profiles for regular player and potential fraudsters or Money Launderers.

8. The directive does not provide a definition of "casino". We understand that this had lead to different treatment of certain gambling activities across Member States. We would be grateful of your views as to whether the directive should be clarified in order to achieve a more consistent approach across the EU?

The most important point is that the (future) directive clarifies the difference between (offline) operators transacting, in cash or equivalent, directly with their clients and those operators who only transact with regulated financial institutions in a traceable (online) environment. The risks are naturally vastly different, especially in regards to the placement

stage of the laundering process. It should preferably also reflect on the various AML risks of the different online gambling products. Given the differences, it is crucial that provisions applicable to non face to face transactions are carried out on a risk sensitive basis and not as high risk basis with automatic enhanced due diligence (EDD).

9. How effective is the current regime for the fight against money laundering and counter terrorism financing, in particular the way it is applied to online gambling and sports betting?

The current AML requirements have worked well to a certain extent. The risks of money laundering and terrorist financing in the online gambling sector are minimal thanks to the transparency and traceability of transactions. As concluded by the Commission workshop on the prevention of fraud and money laundering in June 2011, *“It is not evident that the risks of fraudulent activities and money laundering operations have increased with on-line gambling, as far as regulated gambling markets are concerned.”*

Nevertheless, there is a need to bring more clarity and uniformity in terms of how the directive is being applied to online gambling and betting services.

With reforms of online gambling markets taking place and growing, there is inconsistent implementation and enforcement of the directive – online gambling providers are often licensed in several jurisdictions and these jurisdictions have different requirements in place which are partially putting licensees at business risk. For instance, Italy does not allow its licensors to perform a proactive CDD approach and by this exposes Italian operators to a higher risk to be abused for Money Laundering – not to mention the reputational and financial risk. In France, this is reflected on the different levels of authorities that interfere in AML processes. ARJEL, for instance, in France does expect its licensee to implement proper procedures and controls to detect and prevent Money Laundering (ARJEL regulation) while the data protection authority (CNIL) does not authorize operators to use these procedures and controls. By this, there is an additional risk of not being compliant which highlights that there are loopholes in AML procedures.

Greater focus is also needed on better cooperation. In a number of jurisdictions either no on-line gambling regulations exist or there are weak regulations and the lack of cooperation at international level, including with authorities such as Interpol, gives rise to problems in the cross-border application and enforcement of existing tools, such as customer verification checks.

10. What are your suggestions as to how the rules should be improved?

EGBA recommends the following:

- To acknowledge the vast difference between online and offline casinos and their respective risks
- To clarify the application to online gambling services separately
- To allow CDD requirements to follow a risk based approach

- To have effective CDD requirements suitable for non-cash, non-face-to-face industries
- To take into account the FATF Remote Casino guidelines⁹. In particular, regarding the risk based mechanisms used by the industry for fraud verification such as IP/computer coding verification techniques

⁹ <http://www.fatf-gafi.org/dataoecd/5/61/41584370.pdf>, page 32