The 4th Anti-Money-Laundering Directive and Online Gaming Customer Identification Beyond the Risk-Based Approach

*_By_* „*_Maximilian Riege_*“:http://www.timelaw.de/cms/front_content.php?idcat=50&lang=2, *_salary partner at Hambach & Hambach_*

On 11 March 2014, the European Parliament passed the 4th Anti-Money-Laundering Directive (AMLD).^1^ From a gaming law perspective, a particularly important aspect is the comprehensive inclusion of gaming providers as the addressees of the Directive. Changes regarding the identification obligations for online games have caused criticism.

The original draft of the European Commission for the 4th Anti-Money-Laundering Directive^2^ had provided for a uniform threshold of EUR 2000 for identification obligations for all providers. This threshold applied indiscriminately to terrestrial and to online gaming providers.

In contrast, the version of Art. 10 (1d) of the AMLD, which has now been passed, will lead to different requirements with regard to customer identification depending on the type of game. Whilst terrestrial casinos are only required to identify their customers above a transaction threshold of EUR 2000, and other gaming providers only need to do so if the paid winnings exceed EUR 2000, the identification obligation applies to online gaming providers as early as „upon the commencement of the business relationship“.

Just as the revised German Anti-Money-Laundering Act (GWG),

the different treatment of online games is justified with the allegedly high money-laundering risks associated with online gaming.^3^ In other words: online games are said to be particularly prone to money-laundering activities, whilst terrestrial casinos and other types of gaming are considered to be less suitable in this respect.

This assumption, however, is in contrast to scientific studies and chooses the wrong starting point for the combat of money laundering in the area of gaming. The type of games – whether lotteries, sports bets, casino games or poker, and whether online or offline – is of merely subordinate significance for money-laundering risks. The decisive aspect, rather, is the question of whether or not the gaming offers are regulated or unregulated.^4^

Lower Money-Laundering Risks for Regulated Gaming

As early as 2009, Levi found in his study on „Money Laundering Risks and E-Gaming: A European Overview and Assessment“ that regulated online gaming has hardly any relevance for money-laundering activities. Levi even described the allegation that online gaming is particularly prone to money-laundering, as a myth.^5^ Levi’s view has recently been confirmed by a study compiled on behalf of TÜV Austria Trust IT GmbH. The renowned experts in the area of the combat of money laundering and gaming regulation, Prof. Dr. Dr. h.c. mult. Schneider, Prof. Dr. Dr. Peren and Prof. Dr. Clement, examined the subject „Online Poker: Potential Money Laundering and Its Prevention“.

The results of both of these studies are unambiguous. On the one hand, money laundering in the area of regulated online gaming requires significant efforts, and is thus unattractive under economic aspects.^6^ On the other hand, remaining (residual) risks can be controlled through a „coordinated package of measures“; in this context, Perent/Clement suggest a 10 point plan.^7^

From a criminal’s perspective, money laundering must be worthwhile, i.e. must be economically attractive. Incriminated funds, i.e. funds from criminal activities, are intended to be laundered in order to be re-introduced into the regular economic cycle. Otherwise, proceeds from criminal transactions are of limited benefit for criminals. Furthermore, the money-laundering process is only successful if the funds to be laundered can be re-introduced into the regular economic cycle (so-called integration) after their placement, without too much depreciation loss through the processes applied in order to disguise their origin (so-called layering).^8^ Amounts below EUR 2000 have proven to be irrelevant in view of the efforts associated with the money-laundering activities.

Furthermore, it is particularly easy to monitor the threshold value for deposits and payments especially in the online sector, due to the necessary use of bank transfers or electronic means of payment, excluding the use of cash. The carving up of sums, so-called smurfing,^9^ in order to circumvent the threshold value, is thus far more complicated than in the terrestrial area.^10^

Providers‘ Internal Security Measures

In addition, all gaming transactions can be stored and examined (almost) in real time with regard to anomalies, within the framework of internal security measures taken by the providers, in addition to the registration of the transaction sums, and the payment methods used by the player.^11^

Insofar, the (anonymous) introduction of laundered funds into the regular economic cycle can de facto be prevented, especially for regulated online gaming, through a combination of internal security measures taken by the provider, the restriction of permitted deposits and pay-out methods and sums, as well as the full identification of the customer at the time of a pay-out request.^12^

Section 9a of the German Anti-Money-Laundering Act (GWG)^13^ as well as sections 5 et seq. of the Schleswig-Holstein Decree on the Licensing of Gaming (GGVO) already provide for such measures. Schleswig-Holstein furthermore imposes upon every regulated provider the obligation to install a so-called SAFE server, a mirror server which stores and makes accessible to the competent supervisory authorities all data with gaming relevance (including the transaction data).^14^

This is logical under a number of aspects. Firstly, the supervisory authorities can easily verify compliance with regulatory requirements by the regulated gaming providers. Secondly, storing data creates an additional deterring effect against money-laundering and fraud activities in connection with regulated online gaming. Thirdly, the corresponding criminal activities become unattractive because the discovery risks for criminals as well as the expenses for money-laundering activities are increased significantly. Fourthly and finally, the financial supervisory authority is provided with a reliable calculation basis for the collection of taxes from the regulated providers.

Customer identification vs. channelling

Appropriate identification measures are important to ensure functioning regulation of gaming. This means that a graded, i.e. actually „risk-based“ identification process, is required. If identification standards at the commencement of customer registration are too high, the cumbersome regulation endeavours of the last few years with the aim of attracting players to the regulated market (the so-called channelling of customer demand) could be undermined. Under aspects of regulatory law, high identification obstacles for customers at the beginning of the registration process may even be counter-productive.^15^

Gaming-associated risks can only be controlled within a regulated market. The channelling of customer demand is the

basic requirement for the protection of players and minors, addiction prevention, the combat of money laundering and crime as well as, not least, the generation of tax revenue. These regulatory objectives cannot be achieved, if customers are lost to unregulated gambling offers due to the complexity of the registration process with regulated operators.^16^

In unusual agreement, the authors of the Inter-State Treaty and of the Schleswig-Holstein Gambling Act, stress the special significance of channelling customer demand for the other objectives of gaming regulation, even though they draw different conclusions.

With regard to the 4th Anti-Money-Laundering Directive, this therefore initially results in two possible routes to a solution:

On the EU level, corresponding changes to the AMLD could be agreed during the pending trilogue of European Parliament, European Commission and European Council, in order to prevent an unnecessary and, with high probability, counter-productive identification burden for the regulated online gaming providers at the beginning of customer registration.

On the national level, the competent supervisory bodies of the member states could alleviate the regulatory situation by using the option provided for in Art. 2 (1) No. 3f) of the draft Directive, which is to permit national exceptions from the identification obligation for online gaming, after coordination with the EU Commission. In this context, it would, for instance, be an option to introduce graded identification requirements depending on the sum paid in, a limitation of the permitted payment methods, and payout restrictions.

In particular, in the area of online gaming, a (basic) identification of the customer using his/her bank account data and/or the used EC or credit card will probably suffice for

payments up to certain thresholds, whether at a uniform level of EUR 2000 or with lower minimum amounts. In addition to this, the customer’s (mobile) telephone number could be inquired and verified. The pay-out of funds from a player account should, however, always only take place after a full identification of the customer, and should only be made into a bank account or onto a credit card registered in his/her name.^17^

The customer identification at the beginning of the registration process with regulated online gaming providers must not be to the detriment of the channelling of customer demand into the regulated and thus state-controlled market. Whether or not workable solutions for customer identification can be found which comply with the other objectives of gaming regulation will be decisive for the success of the combat of money laundering under the 4th Anti-Money-Laundering Directive, but also for the success of the regulation of (online) gaming as a whole.

1) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bTA%2bP7-TA- 2014-0191%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

2) http://europa.eu/rapid/press-release_IP-13-87_en.htm.

3) See BT-Drs. 17/10745, 2 et seq.

4) Riege/C. Hambach, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien 2014, Vorb GWG, par. 8 et seq.

5) Levi, Money Laundering Risks and E-Gaming (2009), 26.

6) Schneider, Online Poker: Mögliche Geldwäsche und deren Prävention (2013), 8.

7) Peren/Clement, Online Poker: Mögliche Geldwäsche und deren Prävention (2013), 125.

8) For the 3-phase model, see Herzog, in: Herzog: Geldwäschegesetz (2010), Introduction par. 7 et seq.

9) Herzog, in: Herzog: Geldwäschegesetz (2010), Introduction par. 8.

10) Riege/C. Hambach, in: Streinz/Liesching/Hambach, Glücks- und

Gewinnspielrecht in den Medien (2014), Vorb GWG, par. 9.
11) Riege, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), §9a GWG, par. 4 et seq.
12) Riege/C. Hambach, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), Vorb GWG, par. 13.
13) Riege, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), §9a GWG, par. 5 et seq.
14) Hambach/Riege, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), §§ 4, 5 GlüG SchlH, par. 53 et seq.
15) Riege, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), §9b GWG, par. 16.
16) Hambach/Riege, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), §§ 1-3 GlüG SchlH, par. 11 and 25 et seq.
17) Riege, in: Streinz/Liesching/Hambach, Glücks- und Gewinnspielrecht in den Medien (2014), § 9b GWG, par. 17.