KPMG

AML in the Online Gaming Industry

Prevention of Money Laundering

Background and Scope

The rise of online gaming has brought with it a wealth of opportunities not only for players and operators, but also for crime. The sector's evolution has resulted in a much more complex environment in which it operates. This has led to an increasing difficulty in regulating the sector as well as exposing it to the possibility of criminal exploitation.

Money Laundering & Counter Terrorist Financing in the Sector

Online gaming may be used as a means of laundering funds that have been generated from criminal activities which often involve cross-border organised crimes. Criminals abuse the system by obscuring the link between the funds that have been generated and the original criminal activity. Having a comprehensive compliance programme in place, particularly for anti-money laundering, is not only a legal requirement in most jurisdictions but good business practice in order to protect your company as best possible from any potential criminal activity.

Cybercriminals are constantly looking for new ways to target online businesses in order to facilitate money laundering and the online gaming sector is no exception. Games such as online poker and possessing multiple accounts with the same operator are all ways that money can be laundered. One of the most common occurrences, is where funds are deposited into one account and then withdrawn from a legitimate account in order to mask the original source of the money.

Malta Gaming Authority and AML Prevention

Local legislation is set out in the Prevention of Money Laundering Act (Cap 373, Laws of Malta), which builds on the criminal code (Cap 9, Laws of Malta) and the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR") (collectively, "Anti Money Laundering Legislation"). Together these make up a sound framework for the effective operation of anti-money laundering regulation.

The Malta Gaming Authority (the "MGA"). has set out a number of requirements which must be satisfied by applicants for a Maltese remote gaming application. These requirements are intended to ensure that licensees have the right approach to the prevention of money laundering.

Moreover, local AML regulation requires Maltese licensees to implement a number of anti-money laundering procedures as part of their day-to-day operations.

Obligations and requirements of the licence holder include the following:

- Appoint a designated Money Laundering Reporting Officer (MLRO), whose role is detailed and incorporates the requirements of the local legislator;
- Appoint a designated Key Official who represents the licensee with the MGA and performs a number of key responsibilities;
- To have the following procedures in place:
  - i. Fraud Management procedures;
  - ii. Know Your Client procedures; and
  - iii. Anti-Money Laundering Procedures.

4th EU AML Directive

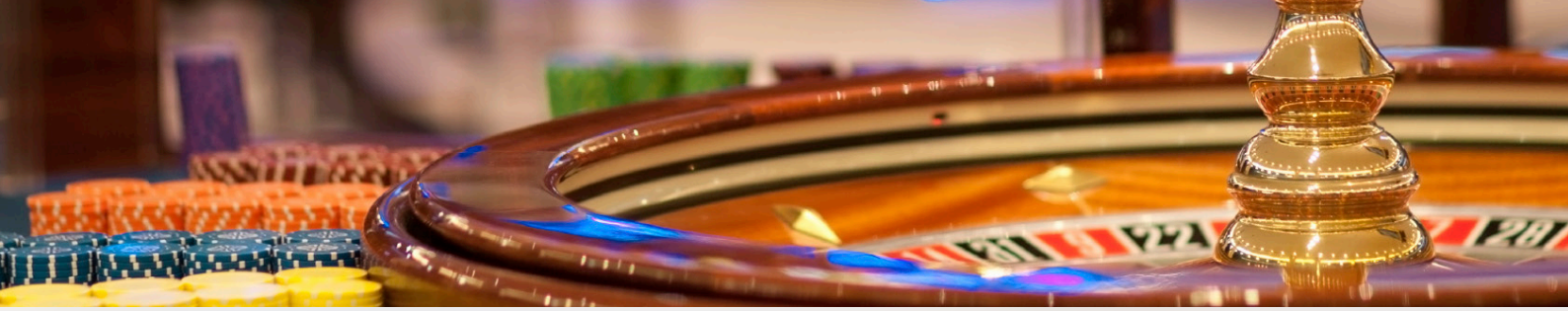
On the 20th of May 2015, the EU Commission adopted new rules to help combat money laundering and terrorist financing in the EU: the 4th Anti- Money Laundering Directive ("the Directive").

The 4th Directive will bring with it significant changes to the AML regime of gambling providers. Gaming will no longer be limited to the definition of land-based casinos but will include all types of "providers of gambling services", aside from those deemed 'low-risk' by the Member State. Some further amendments which will directly affect all gaming providers are the following:

Customer Due Diligence ("CDD")

The 4th Directive has a much wider scope than the currently applicable Directive and expands the circumstances in which CDD should be carried out to include the following:

1. Occasional cash transactions amounting to €10,000 or more in the case of persons trading in goods; and
2. Single transactions of €2,000 or more for providers of gambling services.



The 4th Directive includes a maximum retention period of 5 years for CDD documentation from the end of the business relationship. However this may be extended to a period of 10 years if provided for under local legislation.

Politically Exposed Persons ("PEP")

The 4th Directive clarifies the definition of a PEP and widens the categories of individuals falling under this definition. The 4th Directive requires companies to consider domestic PEPs, in addition to the foreign ones, as high risk clients. Furthermore, companies must perform Enhanced Due Diligence measures with respect to PEPs and are also required to monitor the risk posed by a PEP status for a period of at least 18 months after the time when the PEP chooses to be classified as a PEP, as opposed to the current obligation of 12 months.

Risk Based Approach

Companies are now required to demonstrate that they have taken appropriate steps to identify, assess, understand, and mitigate AML risk and to construct their AML compliance procedures to counter any possible threats.

In this way, companies can allocate and prioritise the appropriate resources to any potential threats detected as well as develop internal policies and procedures that are tailored to their specific requirements. The internal policies and procedures enforced as a result of the risk assessment carried out must also consider factors such as customer, product, geography, and channel..

Beneficial Ownership

The 4th Directive requires that companies hold adequate, accurate and current information regarding their beneficial ownership. This information must be stored on a central register which can be accessed by the authorities and EU Financial Intelligence Units, and others that can demonstrate a legitimate interest. In addition, this requirement will also apply to trustees, who will be required to disclose their status to obliged entities.

Member States must bring into force the laws, regulations and administrative provisions to comply with the 4th Directive by 26 June 2017. Member States may impose more stringent obligations than those outlined in the 4th Directive itself. Firms must now start preparing for compliance with the new rules and will need to consider the effect that the 4th Directive may have on their business.

How can KPMG assist you?

We can assist you in remaining compliant with the ever-changing rules and regulations in order to conduct the best business practise possible and safeguard your company from money laundering and terrorist financing.

KPMG offer a range of service which can be personalised to cater to your specific needs:

- An analysis of your AML/CFT programme to provide you with the reassurance that you are fully-compliant to the latest regulations
- Advice on the creation of AML/CFT regimes
- Provide recommendations on how best to address any identified gaps in line with the legislation
- Provide compliance support to help you understand and asses specific cases.

For further information kindly contact:

Juanita Bencini
Partner, Advisory Services
T: +356 2563 1143
E: juanitabencini@kpmg.com.mt

Alex Azzopardi
Director, Advisory Services
T: +356 2563 1415
E: alexazzopardi@kpmg.com.mt

Raisa Mizzi
Manager, Advisory Services
T: +356 2563 1415
E: raisamizzi@kpmg.com.mt

Russell Mifsud
Senior Manager, Gaming Specialist
T: +356 2563 1044
E: russellmifsud@kpmg.com.mt

Printed in Malta.
February 2016