



EUROPEAN COMMISSION  
 Directorate General Internal Market and Services  
 SERVICES  
 Business-to-consumer services

28 SEP. 2011

Brussels,  
 MARKT E1/CHo/dm (2011) 1122561

## CONCLUSIONS

### WORKSHOP ON ONLINE GAMBLING: PREVENTION OF FRAUD AND MONEY LAUNDERING 1 JULY 2011 IN BRUSSELS

On 1 July, DG Internal Market and Services held the fourth expert-based workshop, complementing the Green Paper on On-line Gambling in the Internal Market with representatives from the relevant sectors: public and commercial gambling operators, gambling regulators and on-line payment service providers. Further to roundtable debates on the pre-determined topics participants agreed on the following conclusions:

#### 1. PROBLEM IDENTIFICATION

On-line gambling is complex in view of its virtual and cross-border nature. However, given the technical systems in place on-line gambling operations are traceable, both in terms of **audit trails of the operations and of the payment systems** with transactions being carried out through financial institutions. Having standards in place means that 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. Competent authorities are to ensure that the inherent technology systems for due diligence controls and audit trails are secured. Money launderers who (manage to) open multiple gaming accounts and reinvest their winnings in different jurisdictions are less easy to track.

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 **cooperation across jurisdictions is key** in fighting these risks. Furthermore, a distinction is to be drawn between licensed and unlicensed operators offering their services in Europe.

In a number of jurisdictions either no on-line gambling regulations exist or there are weak regulations and the **lack of cooperation at the 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, transactions and audit trail integrity.

**Data protection rules** often do not allow for the exchange of information or data, mainly due to confidentiality.

## Type of Fraud

The most frequent type of fraud seems to be **identity theft or bought identities**, a technique that is very often used for money laundering purposes. Match fixing, occurring with the involvement of organised crime structures from non-European jurisdictions is deemed the most severe threat to sport betting operations and the integrity of sport competitions. The frequency and risk of cyber attacks is not considered higher than in any other industry sectors, although this remains a real problem for targeted operators.

Different means of payment (such as credit cards or pay safe cards) may pose different risks in terms of fraud as some may be subject to identity thefts whilst others could be abused for money laundering operations. Operators should deal with the different fraud or money laundering threats within the due diligence checks carried out on customers.

## 2. PREVENTIVE MEASURES

A number of mechanisms have been put in place by operators often due to legal requirements stemming from their licence, such as Know Your Customer (KYC) and Know your Employee (KYE) or imposed by regulators, such as an obligation of regular reporting by the operators and real time monitoring. Nevertheless further concrete measures and standards are deemed necessary.

Whilst a **risk based approach** is favoured, whereby identity monitoring is ongoing and not just on entry, operators are well-aware that this helps mitigate but not eliminate the threats of fraud and money laundering.

**Cooperation** between operators and regulators or voluntary sharing of information was given high importance in the debate. There is also a dire need for tight cooperation with Financial Intelligence Units. Regulators should also be in a position to warn against certain jurisdictions in preventing fraud and money laundering from third country markets.

**Risk assessing** includes identification of jurisdictions into which gambling operations are eventually not offered (either not initiated or suspended). A prevailing challenge for Member States is the fight against illegal gambling.

Conflict of interest rules should be in place in order to prevent match fixing.

In debating the advantages of a clear and consistent approach in Europe to help fight fraud and money laundering, the **Directive on money laundering** was signalled as a concrete example. There is a call to extend this to cover all types of games and to bring it up to date with the online systems. A related topic touched upon is the need to sensitise international enforcement bodies like Europol and Interpol to the underlying criminal nature and scale of the problem.

As regards pay cards, **verification** is to include the destination and not only the funds themselves.

### 3. DETECTIVE MEASURES AND COOPERATION

The **internet facilitates** the detection and subsequent investigation of fraud and money laundering. Detection systems developed in the on-line gambling sector are state-of-the-art technology and are also used in other sectors such as the banking or the insurance sector.

Licensed operators are generally **obliged to report suspicious behaviour** to the regulating authority, such as unusual peaks or uncommon patterns of registered players. This enables the regulating authority to liaise with other operators, mainly to identify commonality of such instances to aid in following up on the reports.

Effective detective measures need to be able to verify the source, the spending behaviour and the destination. A number of early warning systems have been developed by operators and sport federations, but a common constraint is the limited sharing of information, which is seen as restricting the potential of mapping the patterns of suspicious behaviour and identifying the source. It is strongly felt that cooperation and involvement of regulators, police, sports governing bodies and betting operators leads to a positive impact rather than acting in isolation. Rules of sport and rules of betting operators can be better aligned.

**Training** of employees is considered important, and could even be compulsory training. There should also be specific training for example concerning money laundering.

#### **Cooperation and Information Sharing**

Despite the lack of structured cooperation between national gambling authorities, some informal exchange of intelligence exists, between authorities (regulators, enforcement) and with operators. However, more needs to be done in this respect given the complexity of transnational transactions operators and regulators have to face.

There is scope for more cooperation between data protection offices across Member States.

The involvement and joint cooperation with national police authorities and with international enforcement authorities is very important to many of the actors concerned.

Cooperation with banks is also deemed necessary.

The list of participants and the workshop agenda are found at:  
[http://ec.europa.eu/internal\\_market/services/gambling\\_en.htm](http://ec.europa.eu/internal_market/services/gambling_en.htm)